National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-84 (Draft)
Sponsored by the Department of Homeland Security

Guide to Single-Organization IT Exercises

Recommendations of the National Institute of Standards and Technology

Tim Grance
Tamara Nolan
Kristin Burke
Rich Dudley
Gregory White
Travis Good

NIST Special Publication 800-84 (Draft)

Guide to Single-Organization IT Exercises (Draft)

Recommendations of the National Institute of Standards and Technology

Tim Grance
Tamara Nolan
Kristin Burke
Rich Dudley
Gregory White
Travis Good

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2005

U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

Technology Administration

Michelle O'Neill, Acting Under Secretary of
Commerce for Technology

National Institute of Standards and Technology

William A. Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-84 (Draft)
Natl. Inst. Stand. Technol. Spec. Publ. 800-84, 111 pages (August 2005)

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgements

The authors, Tim Grance of the National Institute of Standards and Technology (NIST); Tamara Nolan, Kristin Burke, and Rich Dudley of Booz Allen Hamilton; and Dr. Gregory White and Travis Good of the University of Texas-San Antonio (UTSA); wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would like to acknowledge Joan Hash and Peter Mell of NIST; Dick Broome, Kara Crawley, Courtney Hawkins, Karen Kent, Munir Majdalawieh, and Zara Pyatt of Booz Allen Hamilton; and Dwayne Williams of UTSA for their keen and insightful assistance throughout the development of the document. Additional acknowledgements will be added to the final version of the publication.

The National Institute of Standards and Technology would also like to express its appreciation and thanks to the Department of Homeland Security for its sponsorship and support of NIST SP 800-84.

Table of Contents

List of Appendices

List of Figures

List of Tables

Executive Summary

It is critical for an organization to have plans such as contingency, incident response, and critical infrastructure protection plans in place so that the organization can respond to and manage adverse situations involving information technology (IT). An organization should maintain these plans in a constant state of readiness, which should include having trained personnel able to fulfill their roles and responsibilities; having plans exercised to validate their content; and having systems tested to ensure their operability. These three elements can be carried out efficiently and effectively through the development and implementation of a comprehensive test, training, and exercise (TT&E) program. This document provides guidance on designing, developing, conducting, and evaluating TT&E events so that organizations can improve their ability to prepare for, respond to, manage, and recover from adverse events that may affect their missions. The scope of this document is limited to TT&E events for single organizations, as opposed to large-scale events involving multiple organizations.

As part of creating a comprehensive TT&E program, a TT&E plan should be developed that outlines the steps to be taken. The plan should define the organization's roadmap for ensuring a viable capability, and outline the organization's approach to maintaining plans and enhancing and managing the capability. In addition, the plan should identify resource and budget requirements that enable organizations to achieve an effective, proven capability, and provide a schedule for conducting various types of TT&E events. Creating the TT&E program should also involve several other steps, including developing a TT&E policy, identifying roles and responsibilities, and documenting a TT&E methodology.

The TT&E program should include several types of events to ensure the availability of a wide range of methods for validating various planning elements. Although each type of event has unique characteristics, applying a single methodology to the design, development, conduct, and evaluation of events should facilitate consistency and standardization among events. The types of events covered in this guide are as follows:

- **Training.** Training is a continuum of learning activities that enables staff to maintain and enhance their skills and technical proficiencies and to remain current with technological advances. For the purpose of this publication, training refers only to informing participants of their roles and responsibilities within the plan being exercised, thereby preparing them for tests, exercises, and actual emergency situations. A systematic approach or instructional design model helps ensure that training is designed to meet individual needs, ensure learners' attention spans are not exceeded, and provide the best form of participation. The process assists in providing valuable training events that are designed for the right reasons, for the right audiences, with the right media. Organizations should conduct training sessions as needed, often annually. By conducting training before tests, tabletop exercises, and functional exercises, the organization ensures that its personnel are familiar with their roles and responsibilities within a given plan before exercising the plan itself.

- **Tabletop Exercises.** Tabletop exercises are cost-effective tools for ensuring that plans are viable and implementable in an emergency situation. The objectives of a tabletop exercise are centered on validating the content of the plan, participants' roles and responsibilities as documented in the plan, and the interdependencies documented in the plan. Tabletop exercises are conducted in an informal setting, and a facilitator guides participants through a discussion designed to meet pre-defined objectives. The discussion centers on a single scenario or multiple scenarios. Although typically between 4 and 6 hours in duration, a tabletop exercise can also be conducted on a smaller scale (2 hours) or larger scale (up to 8 hours), depending on the audience, the topic being exercised, and the exercise objectives. The tabletop exercise provides an opportunity for personnel with roles within any given plan to discuss their roles and responsibilities, and also to

identify gaps or shortfalls within the plan before an actual disaster. If conducted regularly, this exercise method provides the means for updating the plan often. Typically, organizations should conduct tabletop exercises semi-annually, following organizational changes, following the issuance of new TT&E guidance, or as needed.

- **Functional Exercises.** Functional exercises provide an opportunity for personnel with operational responsibilities to prepare for adverse events and fully validate the content of their plans and operational readiness in a simulated operational environment. Functional exercises are designed to exercise specific team members, procedures, and assets involved in one or more functional aspects of a plan (i.e., communications, emergency notifications, or IT equipment set-up). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Activities for a functional exercise are scenario-driven and validate the capabilities of an organization to respond to a simulated emergency. The duration of functional exercises varies from between several hours to several days, depending on the event's objectives and the complexity of the plan being exercised. A functional exercise provides personnel the opportunity to identify gaps or shortfalls within the plan before an actual disaster. If conducted regularly, this exercise method provides an effective means for updating plans and familiarizing personnel with their responsibilities. Generally, organizations should conduct functional exercises at least annually or following organizational changes, updates to plans, or the issuance of new guidance.

- **Tests.** Tests are evaluation tools that use quantifiable metrics or expected outcomes to assess the operability of an IT system or IT system component, such as a pager, that is identified as critical in an organization's plans (e.g., contingency plan, incident response plan, critical infrastructure protection plan). A test is conducted in as close to an operational environment as possible, which means that the test should be conducted in a manner that resembles the everyday work environment in which the system or component is found. If possible, an actual test of the components or systems used to conduct daily operations for the organization should be used. Tests can take one of several forms, including component testing (testing individual hardware or software components, or groups of related components); system testing (conducting testing of complete systems to evaluate each system's compliance with specified requirements); and comprehensive testing (testing complete organizations plans such as contingency, incident response, or infrastructure protection plans). A test should be conducted before a system or component becomes operational; after operational use has begun, periodic testing should be conducted to ensure the continued proper and secure use of the system or component. Comprehensive tests of organizational plans should be scheduled periodically to ensure that they are reasonable, effective, and complete, and that all personnel know what their roles are in the conduct of the plan.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

Although it is critical to have plans in place to help an organization respond to and manage various situations involving information technology (IT), it is equally important to maintain these plans in a constant state of readiness. This includes having trained personnel able to fulfill their roles and responsibilities; having plans exercised to validate their content; and having systems tested to ensure their operability. These three elements can be carried out efficiently and effectively through the development and implementation of a comprehensive test, training, and exercise (TT&E) program.

This publication seeks to assist organizations in designing, developing, conducting, and evaluating TT&E events in an effort to aid personnel in preparing for adverse situations. The events are designed to train personnel, exercise plans, and test IT systems, so that an organization can maximize its ability to prepare for, respond to, manage, and recover from disasters that may affect its mission. The guide describes the design, development, conduct, and evaluation of events for single organizations, as opposed to large-scale events that may involve multiple organizations. The vocabulary related to TT&E varies across organizations; this document provides definitions of the terms most commonly used for TT&E-related activities and teams.

1.3 Audience

This document has been created for individuals responsible for their organization's TT&E program. Specifically, the document is designed to assist those responsible for designing, developing, conducting, and/or evaluating events in fulfilling these responsibilities effectively.

1.4 Document Structure

The remainder of this document is organized into five major sections. Section 2 contains information on establishing a TT&E program. Specifically, it describes the need for a TT&E program and the steps involved in creating a TT&E program, including developing a policy; identifying roles, responsibilities, and activities; establishing a schedule; and documenting the methodology.

Section 3 contains information on determining the need for training; creating a training schedule; and designing, developing, conducting, and evaluating the training. This section also describes the design phase in detail, including determining the topic and instructional goals; identifying the performance objectives; determining the assessment tools; identifying instructional strategies, participants, and training staff; and coordinating logistics. Sections 4, 5, and 6 contain similar information for tabletop exercises, functional exercises, and tests, respectively.

This document also contains several appendices. Appendix A provides sample training material. Appendices B, C, and D contain samples of the documentation associated with tabletop exercises, functional exercises, and tests, respectively. Appendix E contains a glossary, and Appendix F contains an acronym list. Appendix G identifies print and online resources that may be helpful in scoping, planning, documenting, conducting, and evaluating TT&E events.

2. Establishing a Test, Training, and Exercise Program

TT&E events are a means for ensuring select personnel are trained in their roles and responsibilities; plans are exercised to validate their viability; and systems are tested to validate their operability. Although an organization could perform only tests, training, or exercises, having a comprehensive program in place that addresses all three areas maximizes an organization's ability to prepare for, respond to, manage, and recover from a disaster affecting the organization's ability to sustain its mission. A comprehensive *TT&E program* defines the organization's roadmap for ensuring a viable capability. The program addresses the organization's approach to maintaining plans, and enhancing and managing a given capability. It also addresses resource and budget requirements that enable the organization to achieve an effective, proven capability, and provides a schedule for conducting various types of TT&E events. This section explains the need for and discusses the steps involved in creating the program.

2.1 The Need for a TT&E Program

A TT&E program should be created in response to Federal guidance recommending that agencies have such programs in place. The program should be coordinated with TT&E guidance documents and practices. Specific guidance documents are as follows:

- Homeland Security Exercise and Evaluation Program Volume III: *Exercise Program Management and Exercise Planning Process*, May 2004[1]
- NIST Special Publication (SP) 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002[2]
- Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations (COOP)*, June 2004[3]
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, February 1996.[4]

TT&E events are major components of plan maintenance. Organizations might have plans in place, but, without exercising them, the organization might never know if the plans are viable and effective. TT&E events provide opportunities for personnel to identify areas with which staff should familiarize themselves more thoroughly, identify gaps or inconsistencies within plans, and identify inoperable or malfunctioning IT systems before an actual event. This early identification of shortfalls allows personnel to identify solutions before an actual adverse event.

2.2 TT&E Program Creation

TT&E programs can be created for various capabilities, but are typically built around an organization's existing plans. It is assumed the organization has developed a plan, and wishes to exercise its validity. It is also assumed that the organization has identified personnel with roles and responsibilities, and wishes to train personnel on their roles and responsibilities under the plan. Finally, it is assumed that the organization has identified systems necessary to perform functions associated with the plan, and wishes to test their operability.

[1] The Homeland Security Exercise and Evaluation Program is available at http://www.ojp.usdoj.gov/odp/docs/HSEEPv3.pdf.

[2] NIST SP 800-34 is available at http://csrc.nist.gov/publications/index.html.

[3] FPC 65 is available at http://www.fema.gov/pdf/library/fpc65_0604.pdf.

[4] Circular A-130 is available at http://www.whitehouse.gov/omb/circulars/a130/a130.html.

Such programs are created for various types of plans, including contingency plans, incident response plans, and critical infrastructure protection (CIP) plans. Table 2-1 lists examples of plans and their focus.

Table 2-1. Examples of Plans

Plan	Focus
Contingency Plan[5]	Sustaining essential functions; resuming/restoring critical business processes; and recovering/reconstituting IT systems
Incident Response Plan[6]	Reporting and managing IT security incidents
Critical Infrastructure Protection Plan[7]	Securing the key infrastructure assets

Regardless of the type of plans an organization has developed, all organizations should have a program in place to validate their plans' effectiveness and to manage the maintenance of the plans. To facilitate establishing a comprehensive program, organizations should first develop a valid TT&E plan that outlines the steps to be taken to ensure the following: personnel are trained in their roles and responsibilities; plans are exercised to validate their content; and IT systems are tested to ensure operability. The TT&E plan outlines all elements of the program, and ensures information surrounding the program is documented. In addition to creating the plan, other major steps in creating a program are as follows:

- Develop overall policy
- Identify roles and responsibilities
- Identify activities
- Establish overall schedule
- Document methodology.

These steps are described in more detail in Sections 2.2.1 through 2.2.5.

2.2.1 Develop Overall TT&E Policy

One of the most critical elements of a viable TT&E capability is a policy that outlines the organization's internal and external requirements associated with training personnel, exercising plans, and testing systems. The purpose of the policy is to ensure that all organizations with planning responsibilities maintain a viable and executable planning capability. The policy forms the framework for the purpose and objectives of the program and cites applicable Federal and internal guidance.

Key steps for developing a TT&E policy are as follows:

[5] Additional information on contingency plans can be found in NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002. Contingency plans include continuity of operations plans, business continuity plans, and disaster recovery plans.

[6] Additional information on incident response can be found in NIST SP 800-61, *Computer Security Incident Handling Guide*, January 2004.

[7] Additional information on critical infrastructure protection can be found in Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 2001.

- Identify all relevant planning documentation (internal and external), such as past training records; organization's policies; Federal guidance; and other practices obtained from other organizations or industry partners

- Collect all governing documentation and maintain the documentation within a central repository

- Update the policy statement as new guidance is applied to or impacts the program.

2.2.2 Identify TT&E Roles and Responsibilities

The office with primary oversight of and responsibility for the TT&E program varies based on the structure or requirements of the organization. In some organizations, oversight and responsibility might lie within the Office of the Chief Information Officer (CIO); in other organizations it might lie within the Management Office. Regardless of which office assumes overall oversight and responsibility, the TT&E program should be managed by a team with direct responsibility for the organization's planning capability. The organization should identify a *plan coordinator* who is responsible for all aspects of planning, including the TT&E element of maintaining the plans. The plan coordinator has overall responsibility for the plan, including development, implementation, and maintenance. One of the plan coordinator's maintenance responsibilities is to identify a *TT&E program coordinator*, who is responsible for developing a plan and coordinating events. Depending on the type of event conducted, the TT&E program coordinator works with design teams, as depicted in Figure 2-1. Sections 3 through 6 contain information on the individual design teams and the roles within each team.

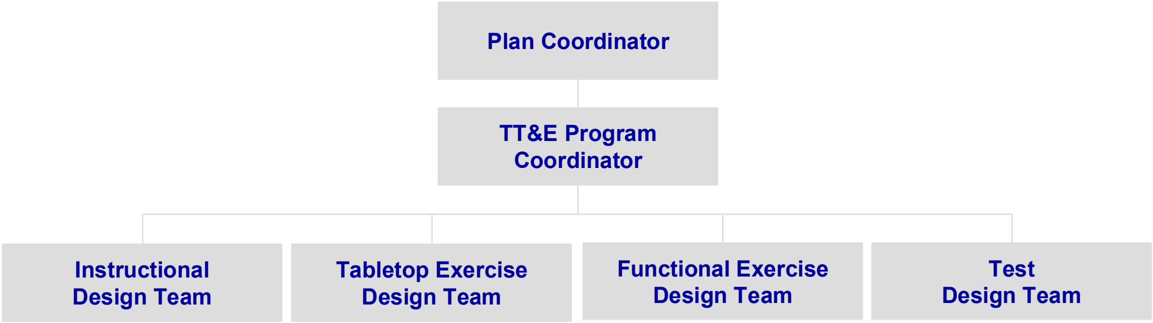

Plan Coordinator
TT&E Program Coordinator
Instructional Design Team
Tabletop Exercise Design Team
Functional Exercise Design Team
Test Design Team

Figure 2-1. Sample Planning Team

2.2.3 Identify TT&E Activities

Although each type of TT&E event has unique components, all are designed to facilitate an organization's ability to prepare for an incident and to have viable, executable plans in place, should the organization be confronted with an emergency situation impacting or threatening to impact the organization's infrastructure, such as cyber terrorism and power failures. An effective program is comprised of training, exercise, and testing events, as follows.[8]

2.2.3.1 Training

Whether the organization is conducting a test, tabletop exercise, or functional exercise, it is critical that the individuals participating in the event are trained in the areas being exercised or tested and in their

[8] Although this guide focuses on single organization exercises, TT&E events can also be performed with multiple organizations.

roles and responsibilities. By ensuring personnel are trained in their roles and responsibilities, personnel are not only prepared to participate in a test or exercise event, but are equally prepared to execute their assigned actions during an actual emergency situation. There are many types of training events, but for the purpose of this publication, training refers only to ensuring personnel are knowledgeable in their roles and responsibilities, including decision making, as assigned in the various plans within the organization.[9]

Training personnel on their roles and responsibilities before an exercise or test event is typically split among two topics: one-third of the training is a presentation on their roles and responsibilities, and two-thirds of the training is activities that allow personnel to demonstrate their understanding of the subject matter and their roles and responsibilities. Section 3 contains detailed information about training events.

2.2.3.2 Tabletop Exercises

Tabletop exercises simulate an emergency situation in an informal, stress-free environment. A scenario is presented to participants, which prompts a discussion focusing on roles, responsibilities, coordination, and decision-making. *Tabletop exercises* are discussion-based events where members of a particular planning team meet in a classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation. A *facilitator* initiates the discussion by asking questions based on the scenario, and keeps the discussion on track to ensure exercise objectives are met. The tabletop exercise is discussion-based only and does not involve deploying equipment or other resources. This exercise method allows for the free exchange of ideas and provides participants an opportunity to identify conflicts or areas of confusion within plans. Section 4 contains detailed information about tabletop exercises.

2.2.3.3 Functional Exercises

Functional exercises provide an opportunity for personnel with operational responsibilities to fully validate the contents of their plans and their operational readiness in a simulated operational environment. *Functional exercises* are designed to exercise specific team members, procedures, and assets involved in one or more functional aspects of a plan (i.e., communications, emergency notifications, or IT equipment set-up). Functional exercises can vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Activities for a functional exercise are scenario-driven and validate the capabilities of an organization to respond to a simulated emergency. Message injects (i.e., a phone call or an e-mail stating that a fire has destroyed the building's IT systems) are used to simulate various aspects of an emergency during a functional exercise. Section 5 contains detailed information about functional exercises.

2.2.3.4 Tests

Tests are evaluation tools that use quantifiable metrics to assess a component or a system in an operational environment specified in the plan. Tests can be performed on a broad range of items from equipment to systems to processes (i.e., testing whether call tree cascades or staff relocation can be executed within prescribed time limits). Due to the quantifiable nature of testing, all tests require the development of a *test plan* that identifies systems or items to be tested, their respective components, and the overall test objectives. Tests can consist of component testing or system testing. "*Component Testing* is testing of individual hardware or software components or groups of related components. *System*

[9] Some types of training events are discussed in detail in NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, and SP 800-50, *Building an Information Technology Security Awareness and Training Program*. Both publications are available for download from http://csrc.nist.gov/publications/nistpubs/index.html.

Testing is testing conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements."[10]

The testing methodology focuses on recovering equipment, testing applications once the equipment is re-established, and establishing backup systems. However, testing varies depending on the goal of the test and its relation to a specific plan. Section 6 contains detailed information about testing.

2.2.4 Establish Overall TT&E Schedule

The TT&E plan should document the projected schedule of activities to be performed within the TT&E program. Although events should be conducted as needed, organizations should evaluate the required frequency of its events and document the frequency of each event in a TT&E schedule. Sections 3 through 6 provide additional detail on how to evaluate the organization's specific TT&E needs.

2.2.5 Document TT&E Methodology

Before implementing the TT&E methodology depicted in Figure 2-2, it is critical that the organization develop a plan that documents the phases to be completed. Although specifics within each phase of the methodology vary based on the type of event conducted, a general methodology is followed for each event. Regardless of the type of event, the methodology includes a design phase, development phase, conduct phase, and evaluation phase. Specific information pertaining to the phases of each event can be found within Sections 3 through 6.

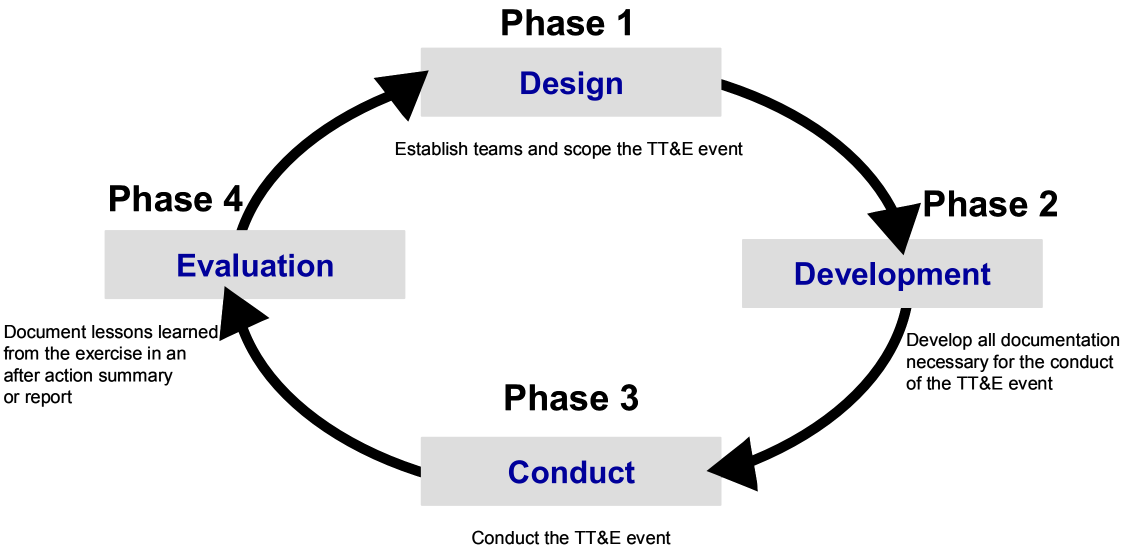

Phase 1
Design
Establish teams and scope the TT&E event
Phase 2
Development
Develop all documentation necessary for the conduct of the TT&E event
Phase 3
Conduct
Conduct the TT&E event
Phase 4
Evaluation
Document lessons learned from the exercise in an after action summary or report

Figure 2-2. TT&E Methodology

2.2.5.1 Design Phase

During the design phase, the TT&E program coordinator works with the plan coordinator to determine the training, exercise, or test topic and scope based on the current needs of the organization. Training topics and scope can range from providing a general overview of the plan to training personnel on their specific roles and responsibilities to training personnel on specific plan components. Tabletop exercise topics can

[10] Institute of Electrical and Electronics Engineers (IEEE). *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. New York, NY: 1990

range from exercising response procedures documented in the plan to exercising decision-making procedures to exercising coordination requirements. Functional exercise topics can include exercising the entire plan or exercising select plan components. Test topics can include testing a specific system or testing system components.

Following the topic and scope selection, the TT&E program coordinator identifies the objectives based on the topic and scope, and identifies who within the organization should participate in the event. The TT&E program coordinator identifies an instructional design team for a training event; a tabletop exercise design team for a tabletop exercise; a functional exercise design team for a functional exercise; or a test design team for a test. The TT&E program coordinator coordinates the event logistics, including document printing; room set-up; meals, if applicable; and audiovisual equipment, if necessary.

2.2.5.2 Development Phase

Upon completion of the design phase, the TT&E program coordinator works with the design teams on the development of the event, which consists of developing the documentation to be used before, during, and after the event. If a training event is conducted, the instructional design team coordinates the development of briefings; assessment tools (activities); participant manuals; instructor guides; and the evaluation criteria to be used when developing an after action summary. If a tabletop exercise is conducted, the tabletop exercise design team coordinates the development of briefing materials; facilitator and participant guides; and the evaluation criteria to be used when developing an after action report. The functional exercise design team coordinates the development of functional exercise material, which varies based the scope of the exercise. It can include an exercise plan (EXPLAN); controller, data collector, simulator, and player briefings; scenario; message injects that comprise a master scenario events list (MSEL); and evaluation criteria to be used when developing an after action report. If a test is conducted, the test design team coordinates the development of a test plan, test scripts, and evaluation criteria to be used when developing an after action report.

2.2.5.3 Conduct Phase

During the conduct phase of a training event, a briefer or trainer typically leads the session by presenting information and facilitating activities related to the topic identified in the design phase. If a tabletop exercise is conducted, a facilitator generally leads a discussion among participants based on the objectives and the scenario, and a data collector captures data. If a functional exercise is conducted, exercise controllers usually direct exercise play, data collectors capture data, and several other exercise positions are staffed to monitor exercise flow. If the organization elects to conduct a test, test administrators normally direct the conduct of the event and data collectors document test results.

2.2.5.4 Evaluation Phase

Following the conduct of a training event, participants typically complete an evaluation/critique form on the success of the event and areas where enhancements can be made in terms of the personnel's knowledge of the trained subject matter. Feedback is analyzed and documented in the after action summary, and future sessions are modified as needed. Following the conduct of an exercise or test, participants typically engage in a facilitated *debrief*, or *hotwash*, to discuss areas that went particularly well and areas where enhancements can be made in terms of the plan's contents and/or the tested systems. Findings discussed during the debrief or hotwash, along with observations made during the course of the event, are documented in the after action report, along with considerations for enhancement.

2.3 Summary

As part of creating a comprehensive TT&E program, it is critical that a TT&E plan be developed that outlines the steps to be taken to ensure personnel are trained in their roles and responsibilities; plans are exercised to validate their contents; and IT systems are tested to ensure their operability. The plan defines the organization's roadmap for ensuring a viable capability, and outlines the organization's approach to maintaining plans and enhancing and managing the capability. In addition, the plan identifies resource and budget requirements that enable organizations to achieve an effective, proven capability, and provides a schedule for conducting various types of TT&E events.

The TT&E program should include events ranging from training sessions to tabletop exercises to functional exercises to tests to ensure the availability of a wide range of methods for validating various planning elements. Although each event has unique characteristics, as identified in Sections 3 through 6, it is important to apply a single methodology to the design, development, conduct, and evaluation of the event. This facilitates consistency and standardization among events.

This page has been left blank intentionally.

3. Training Sessions

Training is a continuum of learning activities that enables staff to maintain and enhance their skills and technical proficiencies and to remain current with technological advances. For the purpose of this publication, training refers only to informing participants of their roles and responsibilities within the plan being exercised, thereby preparing them for tests, tabletop exercises, functional exercises, and actual emergency situations.[11]

This section provides guidance on determining the need for training; creating a training schedule; and designing, developing, conducting, and evaluating training in preparation for a test, an exercise, or an actual emergency situation. The section then summarizes the key elements to consider during and after the conduct of a training event. Appendix A provides a sample curriculum outline and sample training briefing and assessment tools (activities).

3.1 Determine the Need for Training

Within Federal agencies, the need to conduct training is often driven by department or agency requirements, such as the results of audits. The need to conduct training is often driven by the results of a formal needs assessment that has identified specific areas in which personnel should be trained. For the purpose of this publication, it is assumed that the need to conduct training has been determined based either on the results of a needs assessment or on an organization's requirement to conduct training.

3.2 Create a Training Schedule

The training schedule is coordinated closely with the schedules of the other events of the program. Training sessions are conducted as needed (often annually), and typically precede tabletop exercises. By conducting training before tests, tabletop exercises, and functional exercises, the organization ensures that its personnel are familiar with their roles and responsibilities within a given plan before exercising the plan itself.

3.3 Design the Training

The instructional design team[12] designs the training event using a systematic approach. The most common approach is comprised of the following elements: analysis, design, development, implementation, and evaluation. Each step in this process ensures a sound approach to training development and emphasizes quality in the resulting products. Planning for a training event should be started approximately one to two months before the conduct date. Sections 3.3.1 through 3.3.8 describe the major steps in the design process.

3.3.1 Determine the Topic

The TT&E program coordinator determines the training topic based on current personnel requirements identified in Section 3.1. Topic areas include training personnel on, or familiarizing personnel with, their roles and responsibilities within plans, such as contingency plans, incident response plans, and CIP plans. Specific topics range from sustaining essential functions to reporting and managing IT security incidents to securing the key infrastructure assets.

[11] Refer to NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003, for more detailed information on the benefits of training events. It is available for download from http://csrc.nist.gov/publications/nistpubs/index.html.

[12] The instructional design team may consist of one instructional designer or multiple instructional designers, depending on the scope of the training. Instructional designers work closely with subject matter experts (SME) to develop the content.

3.3.2 Determine the Instructional Goal

To determine the instructional goal, the TT&E program coordinator and instructional design team collect and analyze data relating to personnel responsibilities pertaining to the plan to determine tasks, content, and instructional requirements. The instructional goal contains information pertaining to whom will participate, on what topic participants will be trained, and how they will be trained.

3.3.3 Identify the Performance Objectives

The instructional design team defines the process for the topic being learned and specifies how learning occurs. The *performance objectives* define what the learners (or trainees) should be able to accomplish when they have completed each objective in the instructional materials. Performance objectives are important to instructional design because they identify the expected results. Performance objectives are viewed as measurable training, such as what will be performed after completion of the training or which actions will be accomplished once the instruction is completed. The objectives help the instructional design team identify the appropriate level of instruction and help design, implement, and evaluate instruction along with managing the instructional process by determining whether the training was successful. Without writing the performance objectives, the measurable results of the goal cannot be achieved.

3.3.4 Determine the Assessment Tools

The instructional design team designs assessment tools and procedures to provide the evaluation criteria for the instruction as well as the procedures for measuring learner performance. This includes the practice areas and/or activities known as *instruments* that measure participants' performance understanding.

Assessment tools not only measure learner performance, but also the adequacy of the training. The assessment tools help the instructional design team understand the areas of confusion for the learners if the performance objectives are not accomplished and identify what worked well and what needs to be modified based on the results.

3.3.5 Identify the Instructional Strategies

The instructional design team develops the instructional strategies, which effectively and efficiently lead trainee performance. The strategies include sequencing of performance objectives; identifying pre-instructional materials, testing and validating processes, and identifying follow-on activities; determining how the content is presented; and determining participation activities. To ensure transfer of knowledge, skills, or abilities, training events usually are composed of one-third presentation and two-thirds activities.

The instructional design team also selects the media and rationale for delivery to address the practicality and cost effectiveness in terms of the learning context. This step enables the instructional design team to choose the appropriate media for the achievement of the instructional goal (e.g., self study [paper-based or electronic] or classroom).

3.3.6 Identify the Participants

The designer needs to know about the learners and understand their needs. There are many instances where the instructional design team is not involved in the instruction, so they must take the opportunity to learn about the trainees through interviews and/or learner analyses reviews.

All personnel and teams with roles and responsibilities under the plan are invited to participate in the training session. If the primary objective is to validate roles and responsibilities for operational procedures, operational-level personnel should be invited to the training. Once the appropriate participants are identified, they receive a written invitation or announcement of the training/awareness event as soon as possible. This is typically accomplished in the form of an e-mail or memorandum by the TT&E program coordinator.

3.3.7 Identify the Training Staff

The trainer is thoroughly familiar with the content of the training material and works closely with the instructional design team in the development phase. The trainer is informed of the results of previous training events, if applicable, to heighten his or her awareness of potential issues before the training event. Depending on the scope of the event, the training might include multiple trainers and support staff.

3.3.8 Coordinate the Logistics

The instructional design team assigns one to two people (depending on the scope of the event) the responsibility for coordinating the logistics associated with the training event. The logistics coordinator(s) begin to coordinate logistics at least one month before the conduct of the training. The checklist in Table 3-1 can be used by the logistics coordinator(s) to ensure specific logistics considerations are completed:

Table 3-1. Sample Logistics Checklist for Training Events

Logistics	Target Date	Completed
Select a date for training conduct		
Identify trainer		
Determine number of participants		
Invite participants		
Reserve a conference room that accommodates all participants		
Ensure conference room is available one day before the conference to set-up, test equipment, and review graphics		
Determine the need for audio/visual equipment		
Reserve audio/visual equipment		
Arrange for breakfast and/or lunch, if appropriate		
Coordinate the development of the trainer guide and training manuals		
Create a supplies checklist to include items such as plastic nametag holders, power strips, extension cords, scissors, markers, and tape		
Copy all files as a back-up on a CD-ROM, USB flash drive, or other media		
Arrange seating appropriately		
Set up a registration table and place name badges at the registration table		
Place the training manuals on a table either inside or outside the conference room or at individual seats		
Set up, test equipment, and review all electronic materials		
Type attendance roster of participants and provide copies to attendees.		

3.4 Develop the Training

The TT&E program coordinator oversees the development of training and workshop materials. Once the training is designed, the instructional design team assigns roles and responsibilities to the team to develop the training. Training events include the following documentation:

- **Briefing.** The briefing consists of the presentation that is delivered to the participants.
- **Assessment Tools (Activities).** The assessment tools consist of the activities that will allow participants to demonstrate their understanding of the material being presented.
- **Participant Manuals.** The participant manuals include an agenda, briefing materials, workshop activity sheets, acronyms, resources, references, and a point of contact.
- **Instructor Guides.** The instructor's guide generally includes the training performance objectives and goals, briefing materials, discussion points, the related instructional activities and the allotted time frames, and all participant training materials.
- **After Action Summary.** The after action summary is developed after the training event and contains information based on pre-identified evaluation criteria. After action summaries are discussed in Section 3.6.

The instructional materials include the necessary information for each instructional event, including performance objectives, content, practice, and feedback. To start, the instructional design team develops a course outline, and an agenda to include in the curriculum for the training. A sample curriculum outline is located in Appendix A. The instructional design team typically develops the content for the briefing material and assessment tools (activities) identified in the design phase. The instructional design team also develops a detailed instructor's guide and participant manual.

The instructional design team should ensure a process is in place for determining the adequacy of instruction and learning. Evaluation criteria are based on the performance objectives and provide a means to evaluate how well the objectives are met and areas where additional training might be necessary. Conducting an evaluation of training greatly benefits program management and provides invaluable results to the trainees. There are two important phases in the evaluation process: a formative and summative evaluation.

- *Formative evaluation* validates training before implementation. The process includes a review by a subject matter expert not involved in the design process; one-on-one trials; small group practice runs; and/or a field trial. Each part of the process simulates the actual training event to validate timeframes, content, and delivery methods. The process identifies challenges and lessons learned through questionnaires designed specifically for each group in the evaluation. The lessons learned are incorporated into the training documentation before the actual training session.
- *Summative evaluation* validates the training after implementation. The process includes designing an evaluation form with open-ended questions and questions that are rated on a detailed scale. The evaluation forms are distributed to participants at the end of the training session and the information obtained from the forms is captured in an after action summary[13]. After action summaries are discussed in Section 3.6.

[13] NIST SP 800-16 provides a detailed description on evaluating training effectiveness to include the value of evaluation, development of an evaluation plan and behavioral objectives, levels of evaluation, implementation of evaluation planning, and example evaluation forms.

3.5 Conduct the Training

Before the start of the training session, the trainer ensures that the room and registration table have been set up, the participant manuals have been placed at each seat, and all media has been tested. Training is conducted in a classroom-type setting. The U-shaped table is most effective because it permits a trainer to work with each individual or the participants as a group.

During the delivery of the training, a trainer[14] leads the session by presenting information related to the topic identified in the design phase. At the start of the training, the trainer welcomes the participants to the event and requests that the participants introduce themselves by name and provide a general description of their roles within the organization. The trainer then discusses the instructional goal of the training and logistics information. The trainer then walks participants through the training event as designed by the instructional design team using the instructor's guide. The trainer encourages questions and facilitates interaction by administering the activities that prompt participants to work through problems and identify solutions in a discussion-based, team environment.

After the conduct of the training, participants are requested to complete the evaluation/critique form on the success of the event and areas where enhancements can be made in terms of the personnel's knowledge of the trained subject matter. The trainer collects the forms from the participants before the end of the event.

3.6 Evaluate the Training

After the training, the feedback captured in the evaluation/critique forms is analyzed and documented in an after action summary, which is completed within one week following the training. The after action summary contains a graphical analysis of the specific questions in the critique form. Following the summary, future sessions are modified, as needed, or additional training sessions are designed.[15]

3.7 Summary

A systematic approach or instructional design model helps ensure that training is designed to meet individual needs, ensure learners' attention spans are not exceeded, and provide the best form of participation. The process assists in providing valuable training events that are designed for the right reasons, for the right audiences, with the right media.

[14] Depending on the duration and scope of the training event, there could be co-trainers.

[15] NIST SP 800-50 provides additional feedback/evaluation methods and descriptions to include questionnaires, focus groups, selective interviews, independent observation, formal status reports, and benchmarking. The publication also recommends developing a feedback strategy.

This page has been left blank intentionally.

4. Tabletop Exercises

Tabletop exercises are cost-effective tools to validate the content of plans, such as contingency plans, incident response plans, and CIP plans, to ensure the plan content is viable and implementable in an emergency situation. Tabletop exercises are conducted in an informal setting, and a facilitator guides participants through a discussion designed to meet pre-defined objectives. The discussion centers on a single scenario or multiple scenarios. Although typically between 4 and 6 hours in duration, a tabletop exercise can also be conducted on a smaller scale (2 hours) or larger scale (up to 8 hours), depending on the audience, the topic being exercised, and the exercise objectives.

This section provides guidance on evaluating the need for a tabletop exercise; creating a tabletop exercise schedule; and designing, developing, conducting, and evaluating a tabletop exercise. The section then summarizes the key elements to consider before, during, and after the conduct of a tabletop exercise. Appendix B provides a sample tabletop exercise facilitator guide, sample participant guide, and sample after action report.

4.1 Determine the Need for a Tabletop Exercise

To determine the need for a tabletop exercise within an organization, the TT&E program coordinator asks the following questions:

- Have the personnel who would participate in the tabletop exercise been trained on their roles and responsibilities within the plan?
- When was the last time the organization conducted a tabletop exercise?
- Have recent organizational changes impacted the content of the plan?
- Has new TT&E guidance been issued that could impact the content of the plan?

If personnel have not been trained on their roles and responsibilities documented in the plan, the TT&E program coordinator should consider first conducting a training event to maximize the benefits of the tabletop exercise. Personnel trained in their roles and responsibilities participate more effectively in this discussion-based session designed to validate the content of a given plan. If personnel have been trained, conducting a tabletop exercise is the next step to ensuring a viable plan capability.

4.2 Create a Tabletop Exercise Schedule

The tabletop exercise schedule is coordinated closely with the schedules of the other events of the program. The TT&E program coordinator ensures that tabletop exercises are always scheduled within three months after a training event. This ensures that personnel participating in the tabletop exercise are trained in their roles and responsibilities.

Organizations should typically conduct tabletop exercises semi-annually, following organizational changes, following the issuance of new TT&E guidance, or as needed. If personnel have received training and it has been six months since the plan has been exercised, organizational changes have taken place, new guidance has been issued, or the organization has simply deemed a tabletop exercise necessary, it is the appropriate time to conduct a tabletop exercise.

4.3 Design the Tabletop Exercise

Once the need to conduct a tabletop exercise has been established, the TT&E program coordinator typically works with the tabletop exercise design team to design the tabletop exercise event. The design phase is often the most time-consuming phase of the tabletop exercise. Planning for large, complex tabletop exercises should be started at least three months before the desired conduct date. Less complex tabletop exercises should be planned at least one month in advance. Sections 4.3.1 through 4.3.6 describe the major steps in the design process.

4.3.1 Determine the Topics

The tabletop exercise design team characteristically determines the exercise topic based on the plan being exercised. The topic of the exercise will be the same as the focus of the plan. Topics can include contingency planning, incident response, and CIP. Specific topics range from sustaining essential functions to reporting and managing IT security incidents to securing key infrastructure assets. For example, continuity of operations (COOP) plan exercise discussion topics would likely include the roles and responsibilities of personnel with regard to the processes, procedures, and communication and coordination strategies involved in relocating members of the organization’s emergency response group (ERG) to an alternate site; performing essential functions at the alternate site; and accessing vital records and databases at the alternate site. Business continuity plan (BCP) exercise discussion topics would likely include the roles and responsibilities of personnel with regard to the processes and procedures associated with resuming and restoring the organization’s critical business processes. If the organization exercises its incident response plan, topics would likely include processes and procedures for reporting and managing IT security incidents. CIP plan exercise topics would likely include processes and procedures for safeguarding the organization’s infrastructure.

4.3.2 Determine the Scope

The scope of the tabletop exercise is determined based on the target audience. All personnel with responsibilities under the plan should be exercised; however, senior-level teams and operational-level teams should participate in separate tabletop exercises initially due to their different levels of responsibility. Once these two groups have been exercised individually, both groups should participate in a combined exercise to validate coordination between the groups.

The exercise applies to the roles and responsibilities of personnel within the plan being exercised and focuses on validating that the documented roles, responsibilities, and interdependencies are accurate and current. The types of questions asked of the participants during the course of the exercise are tailored to the level of personnel exercised. Senior-level tabletop exercises typically range from two to four hours, while operational-level tabletop exercises range from two to eight hours. Any tabletop lasting beyond four hours in duration should be combined with a training session that precedes the tabletop exercise. If a tabletop exercise is combined with a training session, the event includes briefings, workshops, and hands-on activities in addition to the facilitated session.

4.3.3 Identify the Objectives

The objectives of any tabletop exercise are centered on validating the content of the plan, validating participants’ roles and responsibilities as documented in the plan, and validating the interdependencies documented in the plan. An additional objective is meeting regulatory requirements associated with exercising plans.

4.3.4 Identify the Participants

All personnel and teams with roles and responsibilities under the plan are invited to participate in the exercise. Senior-level personnel and their deputies are invited to participate if the primary exercise objective is to validate the decision-making and oversight processes within the plan. If the primary objective is to validate operational procedures, operational-level personnel are invited to the exercise. If both groups have participated in previous tabletop exercises separately, it is appropriate to conduct a combined session, where senior-level and operational-level personnel discuss individual and team roles and responsibilities and coordination requirements. Once the appropriate participants have been identified, they receive a written invitation or announcement of the exercise as soon as possible. This is typically accomplished in the form of an e-mail or memorandum by a member of the tabletop exercise design team.

4.3.5 Identify the Tabletop Exercise Staff

The tabletop exercise design team usually identifies the facilitator and data collector, who are thoroughly familiar with the content of the plan being exercised and with the exercise objectives. The facilitator and data collector meet with the plan coordinator and tabletop exercise design team before the event to discuss the details surrounding the exercise, including the scope and objectives. At this time, the facilitator and data collector are informed of the results from previous tabletop exercises, if applicable, to heighten their awareness of potential issues before the exercise.

4.3.6 Coordinate the Logistics

The tabletop exercise design team assigns one person on the team the responsibility for coordinating the logistics associated with the tabletop exercise. The logistics coordinator begins to coordinate logistics at least one month before the conduct of the tabletop exercise. The checklist in Table 4-1 can be used by the logistics coordinator to ensure specific logistics considerations are completed.

Table 4-1. Sample Logistics Checklist for Tabletop Exercises

Logistics	Target Date	Completed
Select a date for exercise conduct		
Invite facilitator and data collector		
Invite participants		
Determine number of participants		
Coordinate the development of the facilitator guide and participant guides		
Arrange for the development and printing of name tents		
Reserve a conference room that will accommodate all participants		
Determine the need for audio/visual equipment		
Reserve audio/visual equipment, if applicable		
Arrange for breakfast and/or lunch, if appropriate		
Arrange seating in a u-shape		
Place name tents around the table		

4.4 Develop the Tabletop Exercise

The tabletop exercise involves a minimal amount of documentation. Once the event is designed, the tabletop exercise design team assigns roles and responsibilities to the team to develop the tabletop exercise material. Tabletop exercises include the following documentation:

- **Briefing.** The briefing includes an agenda and logistics information.
- **Facilitator guide.** The facilitator guide includes the purpose for conducting the exercise, scope, objectives, scenario, a list of questions that ensure the objectives are met, and a copy of the plan being exercised.
- **Participant guide.** The participant guide includes the same information as the facilitator guide without the list of questions. Participant guides contain a modified, shorter list of questions to orient participants to the types of issues that are discussed during the exercise.
- **After action report.** An after action report is developed after the exercise event and contains information based on pre-identified evaluation criteria. After action reports are discussed in Section 4.6.

The types of questions documented in the facilitator guide are tailored to the participants. For example, if senior-level personnel are exercised, the questions are of a more general, high-level nature and focus on decision-making and oversight, which are consistent with their roles and responsibilities within the plan. If operational personnel are exercised, the questions are typically focused on specific procedures and processes that are followed to carry out roles and responsibilities.

A common misconception is that scenarios must be very detailed to be effective. In actuality, it is often more effective to develop a short, concise scenario. During tabletop exercises with long, detailed scenarios, participants often spend more time dissecting the scenario and discussing its content then they spend focusing on meeting the objectives. If a detailed scenario is desired, it is critical that a trusted agent, with detailed knowledge of the plan and all the procedures documented within the plan, aids in the development of the scenario to ensure accuracy. In addition, it is essential that the facilitator has the ability to redirect the participants' focus from the scenario to the objectives, should they begin focusing too much on the content of the scenario. Sample tabletop exercise documentation is located in Appendix B.

Evaluation criteria should be developed before the exercise to ensure data collectors know what type of information to capture during the exercise and, ultimately, document in the after action report. Evaluation criteria are based on the exercise objectives and provide a means to evaluate how well exercise objectives were met and identify areas where additional exercises might be necessary.

4.5 Conduct the Tabletop Exercise

Tabletop exercises are conducted in a classroom-type setting, where participants sit around a U-shaped table. The U-shaped table is most effective, because it permits a facilitator to address each individual or the participants as a group while facilitating the exercise. Before the start of the exercise, the facilitator and data collector ensure that the name tents are placed around the table in a manner that will foster communication among participants and teams who work within different operational areas within the organization. Participants are not seated with their teammates. At this time, the facilitator and data collector also place copies of the participant guide with each name tent.[16]

At the start of the exercise, the facilitator welcomes the participants to the event and request that the participants introduce themselves by name and a general description of their roles within the organization. The facilitator then projects the briefing and discusses the scope of the exercise and logistics information. If the tabletop exercise is combined with a training session, the trainer begins the session by providing participants with an overview of the plan and their individual and team roles and responsibilities within the plan.

The facilitator then walks participants through the scenario and kicks off the discussion with one of the discussion questions documented in the facilitator guide, designed to prompt decision-making or coordination among participants. Following the kickoff, the discussion occurs naturally among participants based on the scenario and the objectives. The facilitator may inject periodic questions from the facilitator guide. If the discussion does not occur naturally, the facilitator prompts discussion by asking additional questions from the facilitator guide until all objectives are addressed. If the tabletop exercise is combined with a training event, the facilitator administers hands-on activities before the scenario discussion that prompt participants to work though problems and identify solutions in a discussion-based, team environment. During the course of the exercise, the data collector documents issues to be included in the after action report.

Immediately following the facilitated discussion, the facilitator and data collector conduct an exercise debrief, often referred to as a hotwash. During the debrief, the facilitator asks participants in which areas they excel, in which areas they could use additional training, and which areas of the plan are updated.

4.6 Evaluate the Tabletop Exercise

The comments that surface during the debrief, along with lessons learned documented by the data collector during the exercise, are captured in the after action report, which is typically completed within one or two weeks following the conduct of the exercise. The introduction to the after action reports describes background information about the exercise such as purpose, objectives, participants, and the scenario. The after action report also contains documented observations made by the facilitator and data collector during the exercise and considerations or recommendations for enhancing the plan. Following the development of the after action report, the plan coordinator might assign action items to select personnel in an effort to update the plan being exercised. The plan coordinator then updates the plan, if appropriate, by implementing recommendations made in the after action report.

4.7 Summary

The tabletop exercise provides an opportunity for personnel with roles within any given plan to discuss their roles and responsibilities in an informal environment. The tabletop exercise provides personnel the

[16] Although participants typically receive the participant guides the day of the exercise, the exercise design team may elect to deliver copies of the guide to participants in advance to provide them the opportunity to familiarize themselves with the exercise topic. If the guides are sent in advance, it is recommended that they be sent approximately one week before the exercise. If they are sent too far in advance, the content may be forgotten. If the guides are sent too close to the event, participants might not have an opportunity to read them.

opportunity to identify gaps or shortfalls within the plan before an actual disaster. If conducted regularly, this exercise method provides the means for updating the plan often; thereby, ensuring the plan remains in a constant state of readiness.

5. Functional Exercises

Functional exercises provide an opportunity for personnel with operational responsibilities to prepare for adverse events and fully validate the content of their plans and operational readiness in a simulated operational environment. Functional exercises are designed to exercise specific team members, procedures, and assets involved in one or more functional aspects of a plan (i.e., communications, emergency notifications, or IT equipment set-up). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Activities for a functional exercise are scenario-driven and validate the capabilities of an organization to respond to a simulated emergency. The duration of functional exercises varies from between several hours to several days, depending on the event's objectives and the complexity of the plan being exercised.

This section provides guidance on evaluating the need for a functional exercise; creating a functional exercise schedule; and designing, developing, conducting, and evaluating a functional exercise. The section then summarizes the key elements to consider before, during, and after the conduct of a functional exercise. Appendix C provides functional exercises samples, including a scenario, a tracking form, and an after action report.

5.1 Evaluate the Need for a Functional Exercise

To determine the need for a functional exercise, the TT&E program coordinator considers the organization's overall objectives for conducting a functional exercise and asks the following questions:

- When was the last time the organization conducted a functional exercise?
- Have recent organizational changes impacted the contents of the plan?
- Has new TT&E guidance been issued that could impact the contents of the plan?
- Have the personnel who would participate in the functional exercise been trained on their roles and responsibilities within the plan?
- Have tabletop exercises been held on which potential functional exercises could build?

If personnel have not been trained on their roles and responsibilities documented in the plan, or initial tabletop exercises have not been held to validate the plan's concept of operations, the TT&E program coordinator should consider first conducting a training event and tabletop exercise to maximize the benefits of the functional exercise. If personnel have been trained and the plan has been initially validated through a tabletop exercise, conducting a functional exercise is the next step to ensuring a viable plan capability.

5.2 Create a Functional Exercise Schedule

The functional exercise schedule is coordinated closely with the schedules of the other events of the program. The TT&E program coordinator tries to ensure that functional exercises are scheduled within three months after a tabletop exercise event. This ensures that personnel participating in the functional exercise are trained in their roles and responsibilities and have received an initial tabletop exercise.

Generally, organizations should conduct functional exercises at least annually or following organizational changes, updates to the plan, or the issuance of new guidance. Even after such changes take place, it is usually best to ensure adequate staff training and tabletop exercises have taken place before engaging in a functional exercise.

5.3 Design the Functional Exercise

Once the need to conduct a functional exercise has been established, the TT&E program coordinator typically assigns a functional exercise design team to design the functional exercise. The team is comprised of personnel who are familiar with the plan's content and can facilitate the exercise design process. The design phase of a functional exercise is usually started three to six months before the desired conduct date, depending on the complexity of the exercise. Sections 5.3.1 through 5.3.6 describe the major steps in the design process.

5.3.1 Determine the Topic

The functional exercise design team determines the overarching objectives they have for wanting to exercise a plan. These broad objectives represent the topic areas that will be addressed in the exercise. The topic areas chosen will depend on whether the exercise will address the full plan or specific aspects of the plan. Topic areas addressing the full plan can include but are not limited to validating the plan's procedures, evaluating an organization's ability to implement the plan, and assessing interdependencies of organizations and personnel responsible carrying out the plan. Topic areas that are more narrowly focused on specific aspects of the plan may include assessing the plan's alert and notification process, validating personnel responsibilities associated with the operational phase of the plan, or evaluating the process involved in resuming normal operations.

5.3.2 Determine the Scope

The scope of the functional exercise is determined based on the aspects of the plan to be exercised. The functional exercise design team determines whether only portions of the plan will be exercised or whether all aspects of the plan will be examined. If only portions of the plan are exercised, the functional exercise design team should consider examining a specific phase of plan implementation, such as activation, operation, or reconstitution.

When determining the scope of a functional exercise, the functional exercise design team should clearly identify the specific component or components that will be assessed and consider the types of participants necessary to carry out the exercise. Ultimately, a robust TT&E program ensures that all personnel with responsibilities under the plan are exercised; however, the emphasis of initial functional exercises is often placed on operational-level teams. As an organization's TT&E program matures, senior-level participants also engage in functional exercises to fully validate decision-making and oversight aspects of the plan.

5.3.3 Identify the Objectives

Determining objectives is an important step in designing a functional exercise because the objectives chosen will drive all aspects of designing, developing, conducting, and evaluating the exercise event. The focus of objectives for any functional exercise are centered on validating the content of the plan, validating participants' roles and responsibilities as documented in the plan, providing an opportunity for participants to get hands-on training in executing their functions, validating the interdependencies documented in the plan, and meeting any regulatory requirements associated with exercising plans. Specific objectives derived from the focus areas identified above are to be documented and clearly articulated to exercise participants.

5.3.4 Identify the Participants

Based on the topic, scope, and objectives of the exercise, the functional exercise design team determines who should participate in the event. The participants will be comprised of personnel with roles and responsibilities under the plan and who will be needed to help ensure the exercise meets its stated objectives. For example, senior-level personnel are invited to participate if the primary exercise objective is to validate the decision-making and oversight processes within the plan. If the primary objective is to validate operational procedures, operational-level personnel are invited to the exercise. Once the appropriate participants are identified, they receive a written invitation or announcement of the exercise as soon as possible. This is typically accomplished in the form of an e-mail or memorandum by a member of the functional exercise design team.

5.3.5 Identify the Functional Exercise Staff

The functional exercise design team appoints an *exercise director*, who is responsible for all aspects of the exercise, including staffing, development, conduct, and logistics. The exercise director identifies controllers, data collectors, and simulators, who are thoroughly familiar with the content of the plan being exercised and with the exercise objectives.

The exercise director, controllers, data collectors, and simulators meet with the functional exercise design team before the conduct of the exercise to discuss the details surrounding the exercise, including the scope and objectives. At this time, the exercise director, controllers, simulators, and data collectors review the results from previous tabletop and functional exercises, if applicable, to heighten their awareness of potential issues before the event.

The exercise director also identifies trusted agents, scenario developers, and message inject developers. The *scenario* is a sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives. *Injects* (also referred to as *implementers*) are pre-scripted messages that initiate exercise play. The implementers are the actual items injected by exercise controllers into exercise play. Implementers are usually in the form of messages, letters, memoranda, telephone calls, or radio call scripts. All implementers comprise a *master scenario events list* (MSEL), which is a collection of chronologically sequenced key incidents or activities that participants will be asked to respond to during the course of exercise play.

While the scenario and message inject developers are responsible for developing the scenario and implementers, it is critical that a trusted agent, who has detailed knowledge of the plan and all the procedures documented within the plan, aids in the development of the scenario to ensure accuracy. Additional details on the development of the scenario, MSEL, and injects are provided in Section 5.4.

5.3.6 Coordinate the Logistics

The exercise director assigns one or more team members the responsibility for coordinating the logistics associated with the functional exercise. The logistics coordinator(s) begin to manage logistics approximately three months before the conduct of the functional exercise. The checklist in Table 5-1 can be used by the logistics coordinator(s) to ensure specific logistics considerations are met.

Table 5-1. Sample Logistics Checklist for Functional Exercises

Logistics	Target Date	Completed
Select a date for exercise conduct		
Assign the logistics coordinator(s), and identify controllers, data collectors, and simulators		
Invite participants		
Arrange for the development of controller, data collector, simulator, and participant books		
Coordinate the development of name tags for controllers, data collectors, and simulators to ensure they are readily recognizable during the exercise		
Make arrangements with facility manager(s) at the facilities at which the exercise is conducted		
Arrange for transportation and billeting, if applicable		
Ensure that appropriate equipment is available and properly configured to function at exercise site(s)		
Arrange for breakfast and/or lunch, if appropriate		

5.4 Develop the Functional Exercise

Once the functional exercise is designed, the exercise director assigns roles and responsibilities to the team to develop the exercise. The exercise includes the following documents:

- **Scenario.** The scenario adds realism to the exercise and prompts activities necessary to meet the objectives.
- **MSEL.** The MSEL contains a list of events, key event descriptions, expected actions resulting from the events, and objectives that should be met based on the events.
- **Message Injects.** Message injects contain information designed to supplement the scenario and prompt additional actions.
- **Message Inject Tracking Form.** Message inject tracking forms contain the inject numbers, scheduled times for the messages to be injected into the exercise, actual times that the messages were injected, summaries of the message, and any comments for the individuals injecting the messages.
- **Controller Books.** Controller books contain all information relevant to the controllers during the exercise.
- **Data Collector Books.** Data collector books contain all information relevant to the data collectors during the exercise.
- **Simulator Books.** Simulator books contain all information relevant to the simulators during the exercise.
- **After Action Report.** An after action report is developed after the exercise event and contains information based on pre-identified evaluation criteria. After action reports are discussed in Section 5.6.

Controller, data collector, and simulator books contain the exercise scenario, MSEL, and injects that comprise the bulk of the documentation that is developed in preparation for the conduct of the functional exercise. Scenario and message inject developers are responsible for all aspects of creating the scenario, MSEL, and injects that will be used to direct exercise play.

The scenario is designed to add realism to the exercise by providing participants with situations that will inspire responses that help participants achieve exercise objectives. The scenario chosen should be crafted to adequately address the broad topic areas and specific objectives selected in the design phase. In addition, exercise developers should ensure the scenario does not stray outside the scope of the exercise. Exercise scenarios may be crafted to explore worst-case situations; however, it is often useful to develop scenarios that cause participants to respond to topical issues they are apt to encounter in the real world. For example, an exercise of an IT contingency plan for an organization that is prone to disruptions from natural disasters may consider a scenario involving a significant power outage caused by a hurricane. Other organizations vulnerable to impacts from an explosion at a nearby national security installation may choose a terrorist attack scenario that exercises physical security or evacuation plans. A narrative scenario is documented and distributed to participants via handouts or an oral presentation on the day(s) of the exercise. A sample scenario is provided in Appendix C.

The MSEL serves as an outline of events that will transpire during the course of exercise play. It regulates simulated events by coordinating the actions of participants, defining the schedule of events, and establishing the frequency of message injects. Therefore, the MSEL is planned very carefully to ensure key events lead to the achievement of exercise objectives and ensure that all participants remain active throughout the duration of the event. The MSEL is for exercise development and management purposes only; hence, the list is intended for use by the exercise director, controllers, data collectors, and simulators. A sample MSEL is provided in Appendix C.

Message injects are the actual messages that will be given to players during the course of exercise play. They expand on the outline of key events portrayed in the MSEL; therefore, each MSEL entry may have multiple injects associated with it. The intent of each inject is in concert with the storyline of the overall scenario and MSEL, and prompts a player to take an action that will ultimately lead to achievement of an exercise objective(s). Each inject includes the time at which the message is injected, to whom it will go, from whom the message came, the means by which it will be delivered (i.e., fax, phone, e-mail, etc.), the actual text of the message, and expected actions that participants may take in response to the inject. The number of injects selected should be designed to keep participants adequately occupied but should not be so many that participants will become overwhelmed. Therefore, the number of injects selected will vary based on the duration of the exercise. A sample inject is provided in Appendix C.

Another important aspect of the development phase is determining and documenting exercise evaluation criteria that will be used by data collectors during the conduct of the event. Evaluation criteria are closely tied to the exercise objectives to help data collectors know what type of information to capture during the exercise and ultimately document in an after action report. Once evaluation criteria have been developed, it is often helpful to create forms or other tools that will aid in the data collection process. Such forms instruct data collectors of specific player actions to look for and serve as a roadmap that is used in determining whether specific exercise objectives were achieved, how they were achieved, what improvements may need to be made to the plan that is being evaluated, and where additional exercises might be necessary. After action reports are detailed in Section 5.6.

Functional exercise documentation also includes briefings and/or briefing books for participants, controllers, data collectors, and simulators. Briefings are presented approximately one week before the exercise. The briefings document any information pertaining to the scope and objectives of the exercise, rules of engagement, and administrative aspects of the event. In addition, briefings are conducted to provide controllers, data collectors, and simulators with information pertaining to management aspects of the event, the level of activities that are simulated, and the level of activities that are directed by player action. Each controller, data collector, and simulator receives a book the day of the exercise (or the day of the briefing, if deemed appropriate) containing information pertinent to their roles during the exercise.

5.5 Conduct the Functional Exercise

Functional exercises are typically conducted in real or near-real time and prompt participants to carry out their roles and responsibilities as realistically as possible. A functional exercise is often initiated by a telephone call or other appropriate means, alerting select personnel of the implementation or activation of a specific plan. This alert prompts further notification of all personnel who would be notified via the means identified in the plan. Once the notification process is completed, participants are expected to carry out operational or decision-making activities documented in the plan. Depending on the scope of the exercise, activities could range from carrying out notifications to deploying to an alternate site to mobilizing resources, including staff and equipment. The exercise scope dictates whether deployments or mobilizations are simulated or if they actually occur. If the events are simulated, participants will discuss how they would carry out activities. If the events are not simulated, participants carry out the activities as they would according to the plan being exercised. Participants are informed of any exercise artificialities during the participant briefing.

Controllers, data collectors, and simulators are pre-positioned at the location where the exercise takes place. Controllers form a control cell from which they introduce the scenario and message injects to participants. Controllers administer the exercise by referring to the Inject Tracking Chart and MSEL to ensure the exercise remains on schedule and within scope. A sample Inject Tracking Chart is provided in Appendix C.

The control cell is not typically located in the same work area from which participants carry out exercise activities. Data collectors directly observe player actions during the exercise. They will refer to the evaluation criteria and any other evaluation forms that the data collection team may create to aid their efforts. Simulators assume the roles of various internal and external entities that are not participating in the event, such as government organizations, private citizens, or law enforcement. Information provided by simulators is delivered in accordance with how it would be provided by the organization(s) being simulated. They coordinate closely with the controllers and exercise director to ensure their responses are consistent with the MSEL. Simulators may be collocated with controllers or assemble a response cell in a separate room. During the course of exercise, it is critical that the exercise director, controllers, data collectors, and simulators remain in constant contact with each other. This ensures that the exercise remains coordinated and on schedule.

The exercise director determines when the exercise concludes. Typically, the exercise director ends the exercise when all objectives are met or the MSEL and injects have been fully played out. In cases where a real world emergency occurs, it is the exercise director’s responsibility to call an end to the event. Following the conclusion of exercise play, the exercise director, controllers, and data collectors conduct an exercise debrief with participants, often referred to as a hotwash. The exercise director leads the hotwash and requests feedback from participants, controllers, simulators, and data collectors. Immediately following the exercise, controllers, data collectors, simulators, and participants are asked to provide the exercise director with their notes or any forms completed during the course of the exercise and the hotwash session.

5.6 Evaluate the Functional Exercise

During the evaluation phase, the exercise director relies on data collectors or other specified staff to develop the after action report that documents findings and recommendations from the functional exercise. Exercise notes, forms, and other material created during the course of exercise play and during the hotwash are the basis of the after action report.

The introduction to the after action report documents background information about the exercise such as the scope, objectives, and scenario. Following the introduction, the after action report documents observations made by the controllers, data collectors, simulators, and participants during the exercise and recommendations for enhancing response activities and/or the plan that was exercised. The after action report also includes a list of exercise participants and may provide information from any participant surveys that are distributed during the hotwash. A sample after action report is provided in Appendix C.

The after action report is typically completed within one or two weeks following the conduct of the exercise. In some cases, a Corrective Action Plan is developed during the evaluation phase to provide a roadmap for the coordinator of the plan to aid in updating the plan.

5.7 Summary

Functional exercises provide opportunities for personnel to prepare for adverse events by carrying out their roles and responsibilities in a simulated operational environment. A functional exercise provides personnel the opportunity to identify gaps or shortfalls within the plan before an actual disaster. If conducted regularly, this exercise method provides an effective means for updating plans and familiarizing personnel with their responsibilities, thereby ensuring the organization remains in a constant state of readiness.

This page has been left blank intentionally.

6. Tests

Tests are evaluation tools that use quantifiable metrics or expected outcomes to assess the operability of an IT system or IT system component (e.g., pager, Blackberry) that is identified as critical in the organization's plans (e.g., contingency plan, incident response plan, critical infrastructure protection plan). A test is conducted in as close to an operational environment as possible, which means that the test should be conducted in a manner that resembles the everyday work environment in which the system or component is found. If possible, an actual test of the components or systems used to conduct daily operations for the organization should be used. Before a test is conducted, a test plan should be developed to identify the items to be tested and the objectives for the test. Tests can take one of several forms, including the following:

- **Component Testing.** This involves testing individual hardware or software components, or groups of related components. A component test also might test processes and procedures that are part of any of the organization's plans.
- **System Testing.** System testing is conducted on complete systems to evaluate each system's compliance with specified requirements. A system test should also include an examination of any processes or procedures related to the system being tested.
- **Comprehensive Testing.** This involves the testing of complete organizational plans such as a contingency, incident response, or infrastructure protection plan. These tests generally involve multiple components and systems and may become quite extensive in their scope.

This section provides guidance on evaluating the need for testing; creating a test plan; and designing, developing, conducting, and evaluating a test. The section then summarizes the key elements to consider during a test and after conducting a test.

6.1 Determine the Need for a Test

To determine the need for a component or system test, the TT&E program coordinator should examine all relevant issues, such as the following:

- Is the system or component to be tested installed and ready for operational use?
- Are the processes and procedures for the system or component established?
- Have the personnel been trained on the use of the system or component? How effective has that training been?
- Are there compliance or regulatory issues that mandate certain tests be performed on a specific schedule or frequency?
- When was the last time that this component, system, or plan was tested? Have there been any significant changes or updates since the completion of the last test?

A test should be conducted before a system or component becomes operational, and personnel should be trained on the use of the system or component. If personnel are not trained, system testing should be delayed until they have had a chance to receive appropriate training. Comprehensive tests of organizational plans should be scheduled periodically to ensure that they are reasonable, effective, and complete, as well as to ensure that all personnel know what their roles are in the conduct of the plan.

6.2 Create a Testing Schedule

Before a system or component becomes operational, a test should be conducted to ensure it does not adversely affect the security posture or other operational aspects of the organization. After operational use has begun, periodic testing should be conducted to ensure the continued proper and secure use of the system or component. Testing of organizational plans should be conducted on a regular basis to ensure that the plans are still viable and that all personnel know what their roles are. A high turnover of personnel might necessitate more frequent testing of these plans to maintain the level of preparedness the organization requires.

The scheduling of tests should also consider factors such as available resources. Scheduling comprehensive tests in the summer when many employees are on vacation or during holiday breaks might have a minimal impact on operations but also might limit the number of available personnel. The potential impact on the organization should also be considered. Conducting a test that might affect the operations of the organization might not be wise during known peak operational periods. It is important that when scheduling tests, senior managers are notified and the impact on their operations assessed to determine the best time to conduct the test. Ensuring that senior leadership in the organization has agreed to the test, especially for comprehensive tests, is an essential step in the development of the test.

Testing might also be affected by factors external to the organization itself. Compliance and regulatory issues might dictate certain tests be performed on a specific basis. Scheduling of tests should also include consideration of factors such as environmental issues that might not normally be considered. Scheduling an annual fire or evacuation drill might be better accomplished when the weather is not as harsh, for example, so that employees do not have to stand outside under conditions of extreme temperatures.

6.3 Design the Test

Once a schedule for testing has been determined, the TT&E coordinator should create a test design team[17] to design each specific test. The testing of hardware or software components at the conclusion of their development should also be conducted, but this is not within the scope of this document. Component testing in this document is concerned with individual components already operational that are important enough for the effective operation of the organization that they should be regularly tested. Several factors can have a significant bearing on the design of the test, including the level of the test (component, system, or comprehensive), the organizational entities involved, and the scope of the test. These factors can affect the lead time required to develop the test, the level of complexity for the test, and the length of time the test will take. At an early stage in the design process, the personnel who will participate in the test should be identified and the senior managers for these affected areas should be contacted.

6.3.1 Determine the Scope

The TT&E program coordinator determines the scope of the test based on current system or security requirements and any potential compliance or regulatory requirements. The scope of the test is directly shaped by the level of the test. Component tests are more focused and generally involve fewer individuals and organizational entities. System tests are broader in scope and include more personnel and multiple components. Comprehensive tests involve much larger portions of the organization, potentially including all personnel, and require more extensive coordination and planning.

[17] The test design team should include a team leader and subject matter experts (SME) for each of the areas to be tested; they should develop the content of the test cooperatively.

6.3.2 Identify the Test Objectives

The test design team defines the tests that will be conducted and specifies the expected results or outcomes. The test plan might actually consist of a series of smaller individual tests all designed to examine parts of the component, system, or plan being tested. The objectives for each test should be to measure, check, or verify whether the component, system, or organizational plan satisfies its intended purpose and functions adequately. Where possible, the expected results or outcomes should be expressed in an objective and measurable manner with subjective measurements being avoided. The results should be quantifiable and repeatable to the greatest extent possible.

6.3.3 Determine the Testing Tools

The test design team should specify the assessment tools and procedures needed to accomplish the test. The specific tools needed may vary greatly depending upon the scope of the test. Tools might range from specialized software or hardware tools (e.g., network sniffers, vulnerability scanners) to measurement and recording devices (e.g., stopwatches, cameras, video recorders) to checklists used to measure adherence to defined processes and procedures. Tools might also include items needed for logistical support of the test team (e.g., radios, cell phones, badges).

6.3.4 Identify the Participants

Just as in the selection of the tools needed for the test, the participants might also vary based on the scope of the test to be performed. Participation in testing events can occur at several levels. The first level includes those individuals needed by the design team to help design and conduct the test itself. These individuals are the subject matter experts who help develop the test plan and identify the tools needed, but may not be evaluated in the actual test itself. These individuals would not be considered participants in the exercise, but rather part of the design team who could also be used as observers or facilitators for the test. The second level of participant are those individuals who are operating the components or systems being tested, The third level of participant consists of those individuals who are not directly involved in the test, but who might be impacted by the test or related activities. For example, if the test included an evacuation drill, the involved participants would be all personnel who were forced to evacuate, while affected individuals would include those individuals who might be trying to contact the evacuated people but could not reach them because they were not in their offices. The test design team should attempt to identify all three levels of participants, though the affected individuals might have to be identified as a group, as opposed to individually for comprehensive tests.

6.3.5 Coordinate the Logistics

The test design team assigns overall responsibility for coordinating the logistics associated with the test event to one or two people, depending on the scope of the event. They should begin to coordinate the necessary logistical support far enough in advance to ensure the successful completion of the test. The time required for coordination also depends on the scope, and might vary from a month in advance for component testing to several months for a comprehensive test of a large organizational plan such as a disaster recovery plan. The checklist in Table 6-1 contains examples of possible logistics actions that might need to be performed. Although specific logistical elements are identified during the test design phase, it is imperative that the required list of logistical components be updated frequently. To ensure that all required items are covered. this step should be revisited after the test is fully developed.

Table 6-1. Sample Logistics Checklist for Test Events

Logistics	Target Date	Completed
Select a date for conducting the test(s)		
Identify each individual component that will be tested		
Determine number and type of participants for each test		
Invite core participants to an organizational meeting		
Reserve a conference room that accommodates all participants		
Ensure conference room is available one day before the conference in order to set up, test equipment, and review graphics		
Determine the need for audio/visual and recording equipment		
Reserve required audio/visual and recording equipment		
Arrange for refreshments or meals, if appropriate		
Coordinate the development of the test plan to include expected outcomes and other required documentation		
Create a supplies checklist to include required testing tools, measurement and recording devices, and items such as nametags/nametag holders, clipboards, and pens		
Copy all test documents and files as a back-up on a CD-ROM		
Validate the correct operation of testing equipment and ensure evaluators know how to operate the test equipment		
Coordinate with security personnel and other local officials as required by the test		
Conduct a dry-run/walk through of the test(s) to be performed		
Review procedures to terminate the test, should operational issues dictate the need		
Set up test equipment, and review all electronic materials		

6.4 Develop the Test

Depending on the scope of a test, considerable documentation might need to be developed. This documentation could include the following:

- **Briefings.** For larger system or comprehensive tests, an initial meeting may be used to signal the start of the event. Specific briefings to senior management and to the managers of others that might be affected by the test need to be developed to provide a pre-test understanding for what the test will consist of and why it is important.

- **Test Guide.** This document outlines the basic steps involved in conducting a test and includes a list of the participants. It should also include a list of all individuals and groups who might be affected by the test, and discuss procedures required for early termination of the test should events necessitate this action. This guide provides an overall examination of what will occur during the test.

- **Test Plans.** For each specific test to be performed, a test plan needs to be developed that outlines the specific steps that will be performed. Each step should include a list of required logistical items and should also delineate the expected outcome or response from this step. The procedures for early test termination should be repeated in this documentation, because the evaluators or those people conducting the test should be using the documentation during the test. A list of emergency contact numbers (including cell phone and pager numbers) should also be included.

- **After Action Report.** An after action report is developed after the test is completed. It should contain the results of each individual test as well as an overall synopsis of the test activities. Corrective actions and recommendations are a critical element of this report. For larger tests, an executive summary for senior management should also be created that provides a synopsis of the test, its results, and the recommendations.

6.5 Conduct the Test

With the wide variety of tests that can be conducted, and the vastly different levels of involvement depending on the scope of the test, the settings for tests will vary widely. A small component test could be conducted in a single office, while a complex test of an organizational plan could involve many different parts of an organization in various locations.

When developing a comprehensive test of an organizational plan, there might be significant overlap with what would occur when developing a functional exercise for the same plan. However, a test is conducted in an operational environment whenever possible and is designed to validate the actual effectiveness of both the processes and procedures outlined in the plan, as well as the training that has been conducted, to ensure personnel know how to react and their responsibilities in a given situation. An example of a test for a plan or process might be the traditional fire drill. Do the employees know how to react and where to go? Do they exit the building quickly and efficiently? Were mistakes made that could be prevented through a modification of current plans, processes, training, or technology? Development of a comprehensive test mirrors many of the actions of a functional exercise, including creation of a viable scenario and the development of MSELs and the injects that are used during the test. These items become part of the test plan that is to be followed.

Safety and security are two critical elements that should be maintained during any test. The organization's operational network needs to be protected so that it does not sustain damage. The core function or mission of the organization should not be disrupted to the extent that the organization can no longer function and provide the services that it was created to provide. For these reasons, the test administrator should monitor all tests closely. At any sign of a possible catastrophic disruption, or in the event that the safety of an individual is at stake or the security of the organization or its data might be in question, the test director and any member of the core test team should have the ability to terminate the test immediately.

6.6 Evaluate the Test Results

After the test, the data that has been collected should be evaluated to determine how well the component, system, or plan worked. Were the expected outcomes achieved? Did everything, from both a technical and non-technical perspective, function as expected? What improvements could be made to software, hardware, or procedures? An after action report should be generated that details the results of the test along with any recommendations for improvement. Depending on the scope of the test, this report could take anywhere from a few days to several weeks to prepare. In the event that critical lapses in security or safety are noted, the test director should not wait until the final after action report is created to notify management of these important items. An informal report should be generated immediately with any critical changes that should be made immediately, with the full report following in a reasonable amount of time.

6.7 Summary

Tests are essential mechanisms in ensuring that components, systems, and plans accomplish their intended purposes. Component and system testing can occur as part of a normal development cycle, but may also be used periodically after operational implementation to ensure the continued correct operation of the component. System and comprehensive tests can ensure functional effectiveness in an operational environment. A comprehensive test differs from a functional exercise in that it is performed in as much of the operational environment as possible. This provides a more accurate picture of whether the technologies identified in the plan actually work as intended. Periodic tests are important for an organization to be prepared for events that might otherwise disrupt their operations, and in some cases are mandated by regulation.

Appendix A—Sample Training Documentation

Appendix A provides the following sample documentation:

- Curriculum Outline
- Training Briefing and Assessment Tools (Activities).

This sample documentation is based on training personnel on the use of this guide. Though the content would vary based on the training topic, the format (1/3 presentation, 2/3 activities) should be the same for any training event.

A.1 Curriculum Outline

Title:
[Insert the title of the training and the name of the sponsoring agency.]

Section 1: Introduction
This section provides an outline of the training event. The section includes an objective, the guiding principle, and a description of the intended audience, duration, facilitators, and handouts.

Objective: *[Insert the purpose of the training session to include a description of what is to be learned and how learning will occur.]*

Guiding Principle: *[Insert a description of the why the training event is taking place.]*

Audience: *[Insert a description of the intended target audience.]*

Duration: *[Insert the planned time frame for the training session.]*

Facilitators: *[Insert the name(s) of the agency or company that is conducting the training.]*

Handouts: *[Insert a description of the materials participants will receive at the training event.]*

Section 2: Agenda (optional)
This section provides an agenda and respective time frames if known. The agenda includes the key topics that will be covered during the training event and may be modified as the training materials are developed.

[Insert agenda]

Section 3: Modules
This section provides a description of each module (also known as a unit) to include the purpose, objective, the instructional design team and subject matter expert, and the instructor's name. This section will also include a detailed description of the content in each module that was identified in the training design phase in section 3 of this document.

Module 1 – *[Insert Module Name]*

Purpose - *[Insert module purpose here]*

Objective - *[Insert module objective here]*

Development Team/Subject Matter Expert - *[Insert name of developers here]*
Instructor - *[Insert instructor's name here]*

Content - *[Insert module content information here]*

Module 2 – *[Insert Module Name]*

Purpose - *[Insert module purpose here]*

Objective - *[Insert module objective here]*

Development Team/Subject Matter Expert - *[Insert name of developers here]*
Instructor - *[Insert instructor's name here]*

Content - *[Insert module content information here]*

Module 3 – *[Insert Module Name]*

Purpose - *[Insert module purpose here]*

Objective - *[Insert module objective here]*

Development Team/Subject Matter Expert - *[Insert name of developers here]*
Instructor - *[Insert instructor's name here]*

Content - *[Insert module content information here]*

Module 4 – *[Insert Module Name]*

Purpose - *[Insert module purpose here]*

Objective - *[Insert module objective here]*

Development Team/Subject Matter Expert - *[Insert name of developers here]*
Instructor - *[Insert instructor's name here]*

Content - *[Insert module content information here]*

A.2 Sample Training Briefing and Assessment Tools (Activities)

The following paragraphs provide an outline of topics to cover during a training briefing. Material on the topics should be captured on slides and presented to the personnel being trained during a training event in the form of a slide show. The topic selected for this example is training personnel on how to design, develop, conduct, and evaluate a TT&E event. The text associated with each slide is a sample only.

Slide 1: Test, Training, and Exercise (TT&E) Training Event

Slide 2: Performance Objectives]

After the training, participants should be able to accomplish the following:

- Understand and be able to explain how to determine the need for a TT&E event
- Understand and be able to explain how to create and TT&E schedule
- Understand and be able to explain how to design, develop, conduct, and evaluate TT&E events

Slide 3: Determine the Need for a TT&E Event

- *[Insert the methods for how to determine the need for a training event]*
- *[Insert the methods for how to determine the need for a tabletop exercise]*
- *[Insert the methods for how to determine the need for a functional exercise]*
- *[Insert the methods for how to determine the need for a test]*

Slide 4: Activity One

[Insert an activity that will allow participants to demonstrate their understanding of how to determine the need for a TT&E event]

Slide 5: Create a TT&E Schedule

- *[Insert the methodology for creating a training schedule]*
- *[Insert the methodology for creating a tabletop exercise]*
- *[Insert the methodology for creating a functional exercise schedule]*
- *[Insert the methodology for creating a test schedule]*

Slide 6: Activity Two

[Insert an activity that will allow participants to demonstrate their understanding of how to create a TT&E schedule]

Slide 7: Design a TT&E Event

- *[Insert the process for designing a training event]*
- *[Insert the process for designing a tabletop exercise]*
- *[Insert the process for designing a functional exercise]*
- *[Insert the process for designing a test]*

Slide 8: Activity Three

[Insert an activity that will allow participants to demonstrate their understanding of how to design a TT&E event]

Slide 9: Develop a TT&E Event]

- *[Insert the process for developing a training event]*
- *[Insert the process for developing a tabletop exercise]*
- *[Insert the process for developing a functional exercise]*
- *[Insert the process for developing a test]*

Slide 10: Activity Four

[Insert an activity that will allow participants to demonstrate their understanding of how to develop a TT&E event]

Slide 11: Conduct a TT&E Event

- *[Insert the process for conducting a training event]*
- *[Insert the process for conducting a tabletop exercise]*
- *[Insert the process for conducting a functional* exercise]
- *[Insert the process for conducting a test]*

Slide 12: Activity Five

[Insert an activity that will allow participants to demonstrate their understanding of how to conduct a TT&E event]

Slide 13: Evaluate a TT&E Event

- *[Insert the process for evaluating a training event]*

- *[Insert the process for evaluating a tabletop exercise]*
- *[Insert the process for evaluating a functional exercise]*
- *[Insert the process for evaluating a test]*

Slide 14: Activity Six

[Insert an activity that will allow participants to demonstrate their understanding of how to evaluate a TT&E event]

Appendix B—Sample Tabletop Exercise Documentation

Appendix B provides the following sample documentation:

- Tabletop Exercise Facilitator Guide
- Tabletop Exercise Participant Guide
- Tabletop Exercise After Action Report

This sample documentation is designed to be used as a template by those responsible for designing and developing tabletop exercise documentation. In addition to the documentation described in this appendix, a briefing containing the agenda and logistics information should be developed and projected at the beginning of the exercise.

B.1 Sample Tabletop Exercise Facilitator Guide

[INSERT ORGANIZATION NAME]
[INSERT TABLETOP EXERCISE TITLE]

FACILITATOR GUIDE

[Insert Tabletop Location]

[Insert Tabletop Date]

[Insert table of contents]

SAMPLE INTRODUCTION

In an effort to validate *[insert organization name] [insert name of plan being exercised[18]], [insert organization name]* will conduct a tabletop exercise to examine processes and procedures associated with the implementation of the *[insert plan name]*. This discussion-based exercise will be a *[insert number of hours]*-hour event that will begin at *[insert start time]* and will last until *[insert end time]*.

The exercise is designed to facilitate communication among select personnel regarding the implementation of recovery operations at *[insert organization name]* following an event causing the outage of mission critical systems that are housed in the *[insert facility name]*. This exercise is designed to improve the readiness of the *[insert organization name]* and help validate existing *[insert plan name]* procedures.

Participants should come to the exercise prepared to discuss high-level issues related to the recovery of mission critical systems at the *[insert facility name]*. To achieve the exercise's stated objectives, discussion will focus on the following *[insert facility name]* contingency planning elements:

- What would be done to recover each class of system (e.g., Messaging, Web, Infrastructure) at the [*insert facility name*]?
- How will system recovery be accomplished and what is the priority/optimal chronology of restoration?
- What is the time required for restoration and how can this be optimized?
- What are the expected results and action items that will assist system teams and improve readiness after the exercise?

Participants may choose to bring back-up reference material that will aid in answering the above questions.

SAMPLE CONCEPT OF OPERATIONS

A tabletop exercise is a discussion-based event in which participants meet in a "classroom" setting to address the actions they would take in response to an emergency situation. Tabletops are an effective initial step for personnel to discuss the full range of issues related to a crisis scenario. These exercises provide an excellent forum to examine roles and responsibilities, unearth interdependencies, and evaluate plans.

Participants will be presented with a scenario affecting the *[insert facility name]*. A facilitator will help guide discussion by asking questions designed to address the exercise's objectives. The facilitator may choose to inject modifications to the scenario to further stimulate discussion. Participants will also be encouraged to ask one another questions.

SAMPLE OBJECTIVES

The exercise objectives are as follows:

- Validate the team's ability to recover IT operations at alternate facility

[18] This example illustrates an IT contingency planning tabletop exercise.

- Validate the accuracy of recovery procedures documented in the *[insert plan name]*
- Identify areas of the contingency plan that need to be revised.

SAMPLE AGENDA

Date:	*[insert date]*
Location:	*[insert address]*
9:00 a.m.-9:15 a.m.	Welcoming Remarks and Introductions
9:15 a.m.-9:45 a.m.	Exercise Briefing (Objectives, Rules of Engagement, etc.)
9:45 a.m.-11:30 a.m.	Scenario Discussion
11:30 a.m.-12:00 p.m.	Debrief/Hotwash

SAMPLE SCENARIO

At *[insert time]* on *[insert date]*, an electrical fire in the *[insert facility name]* caused extensive damage and the termination of operations in the data center. The *[insert plan name]* was fully activated in response to this incident, and operations will be conducted at the *[insert alternate facility name]* for the foreseeable future. *[Insert organization name]* employees will be displaced from the building until smoke, water, and other health hazards are removed. Despite the problem at the *[insert facility name]*, Directors and Administrators show no sign of altering their agendas and expect a seamless transition of IT operations to the *[insert alternate facility name]*.

SAMPLE FACILITATOR QUESTIONS

The following questions are designed to be used by the facilitator to guide the discussion and ensure the pre-defined objectives are met; depending on the flow of the exercise, the facilitator may elect to use these questions or other questions to ensure participants meet the objectives through the discussion:

1. Who has authority to activate the *[insert plan name]*?
2. If the plan were activated, what level of staffing should be available at the *[insert facility name]*?
3. How would you be notified of plan activation and by whom?
4. What are the roles and responsibilities of the team at the *[insert facility name]*?
5. How would the transfer of operations have occurred if critical personnel were injured in the fire and could not report to the *[insert facility name]*?
6. Are IT recovery procedures fully documented? Are they accurate? Should additional procedures be documented in the contingency plan?
   - Can recovery procedures be completed within the timeframe dictated in the *[insert plan name]*?
   - What are the steps to reconstitute operations at *[insert facility name]?*

SAMPLE DEBRIEF/HOTWASH QUESTIONS

An after action report identifying strengths and areas where improvements might be made will be provided after the exercise. The following questions are designed to obtain input into the after action report from participants.

- Are there any other issues you would like to discuss that were not raised?
- What are the strengths of the contingency plan? What areas require closer examination?
- Was the exercise beneficial? Did it help prepare you for follow-on testing?
- What did you gain from the exercise?
- How can we improve future exercises and tests?

B.2 Sample Tabletop Exercise Participant Guide

[INSERT ORGANIZATION NAME]
[INSERT TABLETOP EXERCISE TITLE]

PARTICIPANT GUIDE

[Insert Tabletop Location]

[Insert Tabletop Date]

[Insert table of contents]

SAMPLE INTRODUCTION

In an effort to validate *[insert organization name] [insert name of plan being exercised*[19]*], [insert organization name]* will conduct a tabletop exercise to examine processes and procedures associated with the implementation of the *[insert plan name]*. This discussion-based exercise will be a *[insert number of hours]*-hour event that will begin at *[insert start time]* and will last until *[insert end time]*.

The exercise is designed to facilitate communication among select personnel regarding the implementation of recovery operations at *[insert organization name]* following an event causing the outage of mission critical systems that are housed in the *[insert facility name]*. This exercise is designed to improve the readiness of the *[insert organization name]* and help validate existing *[insert plan name]* procedures.

Participants should come to the exercise prepared to discuss high-level issues related to the recovery of mission critical systems at the *[insert facility name]*. To achieve the exercise's stated objectives, discussion will focus on the following *[insert facility name]* contingency planning elements:

- What would be done to recover each class of system (e.g., Messaging, Web, Infrastructure) at the *[insert facility name]*?
- How will system recovery be accomplished and what is the priority/optimal chronology of restoration?
- What is the time required for restoration and how can this be optimized?
- What are the expected results and action items that will assist system teams and improve readiness after the exercise?

Participants may choose to bring back-up reference material that will aid in answering the above questions.

SAMPLE CONCEPT OF OPERATIONS

A tabletop exercise is a discussion-based event in which participants meet in a "classroom" setting to address the actions they would take in response to an emergency situation. Tabletops are an effective initial step for personnel to discuss the full range of issues related to a crisis scenario. These exercises provide an excellent forum to examine roles and responsibilities, unearth interdependencies, and evaluate plans.

Participants will be presented with a scenario affecting the *[insert facility name]*. A facilitator will help guide discussion by asking questions designed to address the exercise's objectives.

SAMPLE OBJECTIVES

The exercise objectives are as follows:

- Validate the team's ability to recover IT operations at alternate facility
- Validate the accuracy of recovery procedures documented in the *[insert plan name]*

[19] This example illustrates an IT contingency planning tabletop exercise.

- Identify areas of the contingency plan that need to be revised.

SAMPLE AGENDA

Date:	*[insert date]*
Location:	*[insert address]*
9:00 a.m.-9:15 a.m.	Welcoming Remarks and Introductions
9:15 a.m.-9:45 a.m.	Exercise Briefing (Objectives, Rules of Engagement, etc.)
9:45 a.m.-11:30 a.m.	Scenario Discussion
11:30 a.m.-12:00 p.m.	Debrief/Hotwash

SAMPLE SCENARIO

At *[insert time]* on *[insert date]*, an electrical fire in the *[insert facility name]* caused extensive damage and the termination of operations in the data center. The *[insert plan name]* was fully activated in response to this incident, and operations will be conducted at the *[insert alternate facility name]* for the foreseeable future. *[Insert organization name]* employees will be displaced from the building until smoke, water, and other health hazards are removed. Despite the problem at the *[insert facility name]*, Directors and Administrators show no sign of altering their agendas and expect a seamless transition of IT operations to the *[insert alternate facility name]*.

SAMPLE PARTICIPANT QUESTIONS

The following questions sample questions that might appear in the Participant Guide.

1. Who has authority to activate the *[insert plan name]*?
2. How would you be notified of plan activation and by whom?
3. Are IT recovery procedures fully documented? Can recovery procedures be completed within the timeframe dictated in the *[insert plan name]*?

SAMPLE DEBRIEF/HOTWASH QUESTIONS

An after action report identifying strengths and areas where improvements might be made will be provided after the exercise. The following questions are designed to obtain input into the after action report from participants.

- Are there any other issues you would like to discuss that were not raised?
- What are the strengths of the contingency plan? What areas require closer examination?
- Was the exercise beneficial? Did it help prepare you for follow-on testing?
- What did you gain from the exercise?
- How can we improve future exercises and tests?

B.3 Sample Tabletop Exercise After Action Report

[INSERT ORGANIZATION NAME]
[INSERT TABLETOP EXERCISE TITLE]

AFTER ACTION REPORT

[Insert Tabletop Location]

[Insert Tabletop Date]

[Insert table of contents]

SAMPLE INTRODUCTION

On *[insert date]*, *[insert organization name]* participated in *[insert duration of exercise]*-hour tabletop exercise designed to validate their understanding of the *[insert plan name]*.

SAMPLE OBJECTIVES

The exercise objectives are as follows:

- Validate the team's ability to recover IT operations at alternate facility
- Validate the accuracy of recovery procedures documented in the [insert plan name]
- Identify areas of the contingency plan that need to be revised.

SAMPLE AGENDA

Date:	*[insert date]*
Location:	*[insert address]*
9:00 a.m.-9:15 a.m.	Welcoming Remarks and Introductions
9:15 a.m.-9:45 a.m.	Exercise Briefing (Objectives, Rules of Engagement, etc.)
9:45 a.m.-11:30 a.m.	Scenario Discussion
11:30 a.m.-12:00 p.m.	Debrief/Hotwash

SAMPLE DISCUSSION FINDINGS

The *[insert exercise name]* provided information on *[insert relevant information]*. An important benefit of the exercise was the opportunity for participants to raise important questions, concerns, and issues. At the conclusion of the exercise, participants were asked to complete an evaluation form regarding the information provided, additional information needed, and their thoughts on the event and topics, to be included in the after action report. *A sample evaluation form can be found on page C-16.*

The discussion findings from the exercise along with any necessary recommended actions are as follows:

General Findings

The exercise provided an excellent opportunity for participants to *[insert relevant information]*. As a result of the exercise, participants left with a heightened awareness of *[insert relevant information]*.

Specific Findings

Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:

Observation 1. [Insert general topic area]

[Insert observation]

Recommendations

[Insert recommendations]

Observation 2. [Insert general topic area]

[Insert observation]

Recommendations

[Insert recommendations]

Example Observations and Recommendations:

Observation 1. Communications

A plan identifying standardized systems for communicating with contingency plan members does not exist.

Recommendations

- The organization should consider developing a communications plan that establishes standardized communications requirements, addresses how and where backup communication systems will be positioned, and describes procedures for personnel to access backup communication systems.
- The organization should identify redundant communications systems to ensure that essential personnel can be contacted in the event of an emergency. Redundant communications systems may consist of home telephones, cellular telephones, laptop computers, and other communications systems.

Observation 2. Flyaway Kits

Essential personnel have not been issued flyaway kits, containing personal items and/or those items needed to perform their operations, to carry to relocation facilities in the event of an emergency.

Recommendation

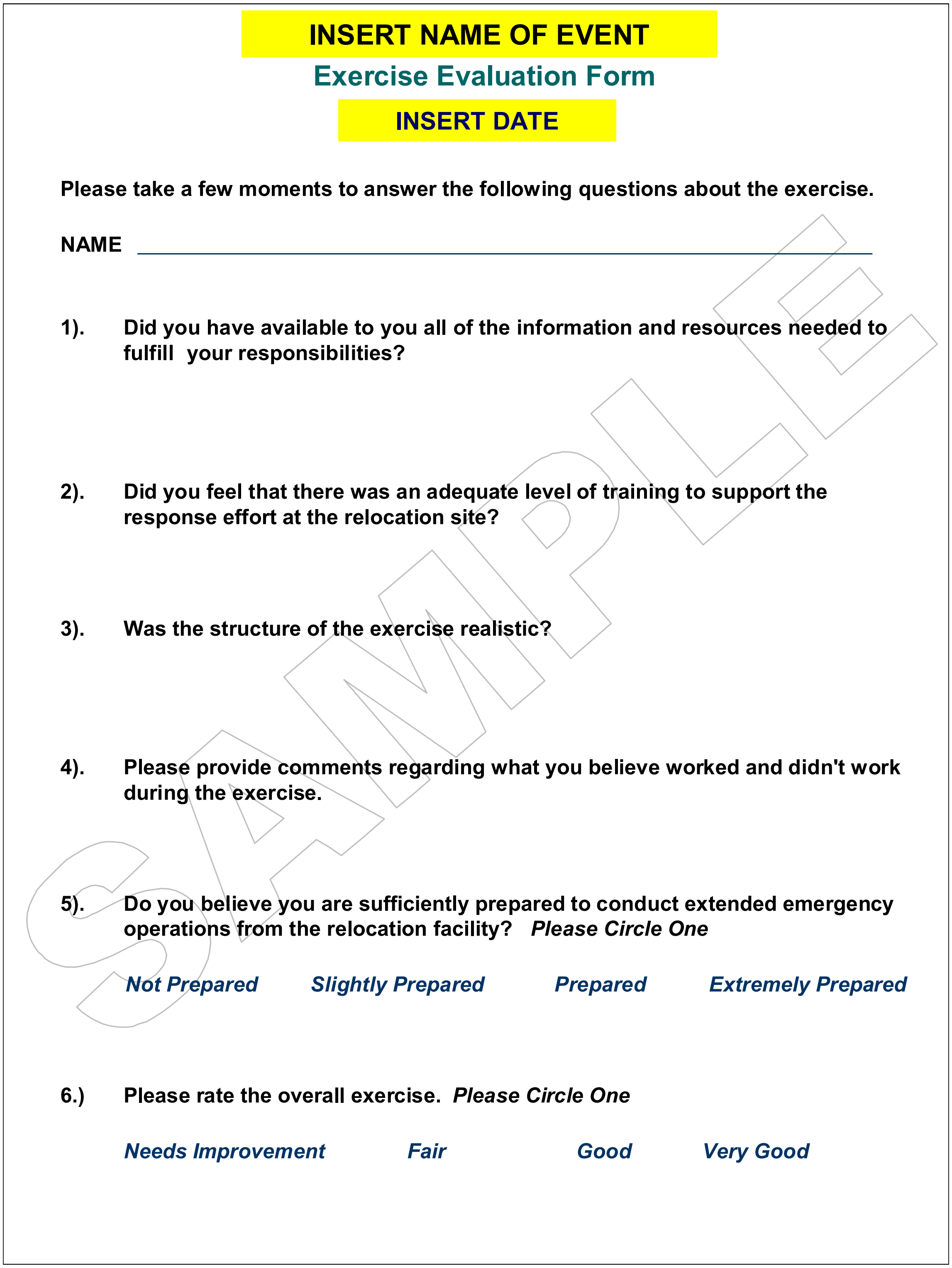
- The agency should examine the possibility of developing flyaway kits and distributing them in advance to personnel who would relocate during an emergency. In addition to personal items that personnel might need if deployed for an extended period of time, flyaway kits should contain flash drives, diskettes or CD-ROMs with information needed for essential personnel to carry out their essential functions.

SAMPLE SIGN-IN SHEET

Participant	Function/Title	Telephone Number/ E-mail Address

SAMPLE EVALUATION FORM

Please take a moment to fill out the evaluation form.



INSERT NAME OF EVENT

Exercise Evaluation Form

INSERT DATE

Please take a few moments to answer the following questions about the exercise.

NAME ____

1). **Did you have available to you all of the information and resources needed to fulfill your responsibilities?**

2). **Did you feel that there was an adequate level of training to support the response effort at the relocation site?**

3). **Was the structure of the exercise realistic?**

4). **Please provide comments regarding what you believe worked and didn't work during the exercise.**

5). **Do you believe you are sufficiently prepared to conduct extended emergency operations from the relocation facility?** ***Please Circle One***

Not Prepared ***Slightly Prepared*** ***Prepared*** ***Extremely Prepared***

6.) **Please rate the overall exercise.** ***Please Circle One***

Needs Improvement ***Fair*** ***Good*** ***Very Good***

SAMPLE EVALUATION RESULTS

Following the *[insert tabletop exercise name]*, on *[insert date]*, participants were given an evaluation form on which to record their impressions of the exercise. These forms allowed participants to rate presentations on a numerical scale and to provide additional comments for consideration in the after action report. Refer to Exhibit 1 for more detailed information regarding the participants' responses. *Each exhibit will reflect the evaluation forms for each individual event. If evaluation forms have a point scale, either a pie chart or bar graph will be depicted.*

The questions covered whether participants thought additional issues should have been raised; whether participants thought the exercise was beneficial; what participants gained from the exercise; and what can be done to improve future exercises. *[Insert percentage]* of the participants completed the evaluation.

In response to the question regarding whether participants thought additional issues should have been raised, nearly *[Insert percentage]* of those who completed the evaluation indicated that all relevant issues were addressed. Other comments were *[insert relevant information]*.

In response to the question regarding whether participants thought the exercise was beneficial, *[Insert percentage]* of those who completed the evaluation indicated that the exercise was beneficial. Comments ranged from *[insert relevant information (i.e., "good start" to "extremely beneficial.")]*.

In response to the question about what participants gained from the exercise, nearly *[Insert percentage]* of those who completed the evaluation form remarked *[insert relevant information]*.

EXHIBIT: PARTICIPANT RESPONSES

What are your thoughts on the exercise?	What did you gain from the exercise?
■ *[Insert comments]* ■ ■ ■	■ *[Insert comments]* ■ ■ ■

Overall, the feedback from the *[insert tabletop exercise name]* was *[insert relevant information]*.

This page has been left blank intentionally.

Appendix C—Sample Functional Exercise Documentation

Appendix C provides the following sample documentation:

- Scenario
- Master Scenario Events List (MSEL)
- Message Inject
- Message Inject Tracking Form
- After Action Report.

This sample documentation is designed to be used as a template by those responsible for designing and developing functional exercise documentation. In addition to the documentation described in this appendix, a briefing containing the agenda and logistics information should be developed and presented at the beginning of the exercise.

C.1 Sample Functional Exercise Scenario

[INSERT ORGANIZATION NAME]
[INSERT FUNCTIONAL EXERCISE TITLE]

SCENARIO

[Insert Functional Exercise Location]

[Insert Functional Exercise Date]

The scenario is developed by the functional exercise team during the Development Phase. Scenario documentation may include a brief Scenario Background designed to provide participants a sense of the world/local situation in the weeks or months before the start of the exercise. This information will be provided to participants in briefings before the exercise or at the beginning of the exercise event. The scenario itself portrays the events that will occur during the conduct of the event. These events will also become a part of the Master Scenario Events List and will be introduced into exercise play in the form of Injects.

SAMPLE SCENARIO BACKGROUND

D-Day Minus 20

International tensions have dramatically risen overseas involving strategic interests of the United States. Despite attempts to resolve disputes diplomatically, troops from hostile countries deploy and appear poised to make a major military incursion against nations allied to the United States. U.S. intelligence agencies also detect documented attempts by hostile nations to destabilize the governments and economies of allies, which would have an adverse impact on U.S. military and economic interests in the region.

D-Day Minus 10

As tensions continued to build, hostile entities undertake small-scale military operations against allied and U.S. interests overseas. A U.S. reconnaissance plane is shot down and the bodies of the dead crew are displayed on television. An emergency Cabinet meeting is called and it is decided that the U.S. military will deploy to the region to protect allied governments and U.S. interests. It is anticipated that an initial operational capability to defend U.S. interests will not be complete until next month.

D-Day Minus 5

In response to the U.S. declaration to send troops and materiel to the region, hostile nations vow to take whatever actions are necessary to “strike a vicious blow against the American imperialists.” They state that any war that the U.S. provokes will also be fought on the American homeland. U.S. intelligence agencies soon detect an increase of cyber attacks against U.S. critical infrastructures and threats to carry out terrorist attacks against the U.S. government. Intelligence also indicates that hostile foreign interests within the U.S. are increasingly active and terrorist cells in other countries have been activated to potentially carry out attacks against the U.S., both overseas and within U.S. borders. U.S. government officials suspect that the hostile nations hope to weaken U.S. public support and impede the military’s capability to deploy by engaging in actions that might include the use of weapons of mass destruction and cyberterrorism. Nevertheless, the U.S. military continues to deploy to the region.

SAMPLE SCENARIO

D-Day

0900: The United States Computer Emergency Readiness Team (US-CERT) issues an alert indicating the presence of what is thought to be an advanced computer worm. US-CERT estimates that the worm has already infected over 500,000 computers worldwide in only 2 hours, prompting the center to warn that the worm's spread has the potential to disrupt business and personal use of the Internet for applications such as electronic commerce, e-mail, and entertainment. U.S. intelligence agencies link the worm's release as a response to U.S. military deployments and fear the attack may have been designed specifically to disrupt communications between agencies supporting the military deployment.

Intrusions into numerous Federal Web sites have been reported in recent hours. Hackers, who government officials believe to be associated with hostile nations, have successfully compromised the security of various U.S. Government information systems. Anti-government vandalism has also been reported on numerous department and agency Web sites.

[*Insert organization/data center name*] is currently in the process of responding to the effects of the worm and defending against further electronic intrusions.

1000: As a result of credible threats of imminent terrorism and the fear that ongoing electronic intrusions against Federal information systems may be part of a concerted information warfare attack, the Department of Homeland Security (DHS) raises the Homeland Security Advisory System threat condition from an Orange "High" to a Red "Severe" risk of terrorist attack.

1200: A freight train pulling numerous tanker cars passes slowly through the center of the city. Some of the tankers are carrying methyl isocyanate (MIC), a highly explosive chemical used in the production of pesticides. As the train passes the [*insert name of organization's facility*], one of the tanker cars erupts in a violent explosion. The blast collapses a portion of the building and results in power outages in the immediate vicinity. Many personnel in the [*insert name of organization's facility*] are killed or injured.

The [i*nsert data center name*] survived the blast and emergency power was engaged for critical IT systems. Several data center personnel had recently left the center for lunch and their well-being is unknown at this time. Management has directed that the data center implement contingency plans and relocate to their alternate computing facility. In addition to restoring essential data center operations at the alternate facility, management indicates that defending [i*nsert organization name*] from further electronic intrusions remains a priority.

D-Day Plus 1

1000: Intelligence and law enforcement agencies continue to track numerous threats against the United States. The Federal Bureau of Investigation (FBI) notifies Government agencies of documented threats of further attacks against Federal departments and agencies and critical infrastructure facilities throughout the United States. One such notice to [i*nsert organization name*] includes a report of possible terrorist surveillance activities outside the organization's alternate computing facility. As a result, management directs that data center personnel explore options to move operations to a backup alternate facility in the event that the threat is found to be credible.

C.2 Sample Functional Exercise Master Scenario Events List

[INSERT ORGANIZATION NAME]
[INSERT FUNCTIONAL EXERCISE TITLE]

MASTER SCENARIO EVENTS LIST (MSEL)

[Insert Functional Exercise Location]

[Insert Functional Exercise Date]

The Master Scenario Events List (MSEL) is created by the functional exercise team during the Development Phase. The MSEL lists key scenario events, expected Injects that will build on the key events, and the objectives of the each MSEL item. Controllers, simulators, and data collectors will refer to the MSEL throughout the Conduct Phase of the exercise to ensure the exercise remains on track.

Master Scenario Events List

Event #	MSEL Key Event Description	Expected Actions Resulting from MSEL Event	Objectives
1	***Example*** The [*insert organization name*] experiences electronic intrusions on critical information systems.	***Example*** Supporting Injects: Day 1, 0900 - 1700 ■ Activate cyber incident response team ■ Implement Cyber Intrusion Response Plan ■ Notify and coordinate with customers and other stakeholders ■ Take actions to clean infected systems	***Example*** ■ Familiarize staff with responsibilities under Cyber Intrusion Response Plan ■ Validate Cyber Intrusion Response Plan ■ Coordinate with Federal cyber entities, customers, and key stakeholders
2	***Example*** The Homeland Security Advisory System threat level has been raised from an Orange “High” to a Red “Severe” risk of terrorist attack.	***Example*** Supporting Injects: Day 1, 1000 - 1200 ■ Activate emergency response teams ■ Initiate backup procedures for all mission critical IT systems ■ Relocate essential personnel to alternate facilities ■ Coordinate with the White House and other departments and agencies to inform them of decision to relocate operations	***Example*** ■ Familiarize staff with emergency activation and notification procedures ■ Validate IT contingency plans and procedures ■ Validate relocation plans and procedures ■ Validate coordination and communications processes with key stakeholders
3	***Example*** A large explosion occurs outside the Office Building.	***Example*** Supporting Injects: Day 1, 1200-1700 ■ All commercial power to building has been cut ■ The site reports that some data communications links have failed ■ Facility managers report the building cannot be repaired	***Example*** ■ Validate IT contingency plans and procedures ■ Identify whether additional contingency plans need to be developed ■ Examine plans to restore data center operations
4	***Example*** Possible threat of terrorism to alternate facility.	***Example*** Supporting Injects: Day 2, 1000-1200 ■ Explore options if alternate facility is disabled ■ Prioritize IT system recovery	***Example*** ■ Identify whether additional contingency plans should be developed for alternate facility

C.3 Sample Functional Exercise Injects

[INSERT ORGANIZATION NAME]
[INSERT FUNCTIONAL EXERCISE TITLE]

INJECTS

[Insert Functional Exercise Location]

[Insert Functional Exercise Date]

Injects are created by the functional exercise team during the Development Phase. These messages are introduced by Controllers during the Conduct Phase and are provided to exercise participants via the means shown on the Inject form. In the case of the Sample Inject provide below, a Controller would play the role of the Chief Information Officer and would call the Team Chief to provide information and request follow-on action. Expected actions by the Team Chief or other exercise participants are documented in the "Notes to Control/Response Cell" at the bottom of this form to aid controllers, simulators, or data collectors in anticipating what actions will result from the Inject.

****EXERCISE**EXERCISE**EXERCISE**EXERCISE****

[Insert Name of Exercise]
Implementers for *[Insert Date]*

EXAMPLE

#15 – [*Insert inject title*] **(i.e., Development of Disaster Recovery Strategies for Alternate Facility)**

Inject Date/Time: [*Insert date/time*] **(i.e., Day 2, 1045)**

From: [*Insert by whom the message is delivered*] **(i.e., Chief Information Officer)**

To: [*Insert for whom the message is intended*] **(i.e., Team Chief)**

Inject Means: [*Insert the means by which the message is delivered*] **(i.e., Phone Call)]**

[*Insert message text*]

Example

Now that we know the magnitude of the damage to the Building and our data center there, it is apparent that we will be operating out of the alternate facility (AF) for the foreseeable future. Given the continued threat of terrorist attacks, we need to develop contingency plans in the event of a major outage affecting the AF. What is our strategy to ensure continuity of mission critical systems at the AF? Which systems and applications are prioritized for recovery? How long will it take to develop a viable backup for those systems?

Note to Control/Response Cell:

[*Insert any type of information that the Control/Response Cell may need to consider to track, evaluate, or respond to exercise players*]

Example

Expect the AF Team Chief to consult the AF Contingency Plan and coordinate with appropriate system and application engineers to develop a recovery strategy.

C.4 Sample Functional Exercise Inject Tracking Form

[INSERT ORGANIZATION NAME]
[INSERT FUNCTIONAL EXERCISE TITLE]

INJECT TRACKING FORM

[Insert Functional Exercise Location]

[Insert Functional Exercise Date]

Portions of the Inject Tracking Chart are developed by the functional exercise team during the Development Phase, and additional information is filled in by Controllers during the Conduct Phase. In the sample below, ***BOLDED*** *text would have been created during the Development Phase and ITALICIZED text would have added to the chart by Controllers during the Conduct Phase. The purpose of the form is to provide Controllers with a "play book" that states which injects are provided to participants at each given time. The form is then used by Controllers to document the time at which an Inject is introduced and a summary of activities taken by participants in response to the Inject.*

Inject Tracking Chart				
Inject #	**Scheduled Inject Time**	**Actual Inject Time**	**Inject Summary**	**Comments**
Example **1**	*Example* **0900**	*Example* *0901*	*Example* **Malicious Computer Worm Denial-Of-Service Attacks**	*Example* *Injected by Director to Chief. Chief assigned immediate action to Network Administrator. Administrator took appropriate actions and informed management and customer advocate. Administrator continued to monitor developments for remainder of exercise.*
Example **2**	*Example* **1015**	*Example* *1018*	*Example* **Situation Reporting Schedule to Leadership**	*Example* *Injected by Director to Chief. Chief assigned action to Operations Officer at 1020, who logged and posted schedule for all of team per standard operating procedures.*
Example **3**	*Example* **1025**		*Example* **Call to White House**	
Example **4**	*Example* **1200**		*Example* **Large Explosion Outside Office Building**	

C.5 Sample Functional Exercise After Action Report

[INSERT ORGANIZATION NAME]
[INSERT FUNCTIONAL EXERCISE TITLE]

AFTER ACTION REPORT

[Insert Functional Exercise Location]

[Insert Functional Exercise Date]

The After Action Report is developed by Data Collectors during the Evaluation Phase. The After Action Report provides relevant background information about the event, scope of the exercise, objectives, scenario, and key findings and recommendations. In addition, the After Action Report lists the event's participants and may provide relevant information from surveys completed by participants at the conclusion of the exercise.

SAMPLE TABLE OF CONTENTS

[Insert table of contents]

SAMPLE INTRODUCTION

On *[insert date]*, *[insert organization name]* participated in *[insert duration of exercise]* functional exercise designed to validate their understanding of the Cyber Intrusion Response Plan and the Alternate Facility Contingency Plan. *[Insert any other additional background information about the exercise that is relevant for the after action report.]*

SAMPLE SCOPE

The exercise was designed to examine the *[insert organization's name]* ability to respond to a concerted cyber attack campaign from the alternate computing facility. The event examined all aspects of the activation, operation, and reconstitution phases of both the Cyber Intrusion Response Plan and the Alternate Facility Contingency Plan. All personnel with operational responsibilities under the two plans participated in the event. Senior level decision-makers were not exercised in the exercise; however, a second exercise focused on management activities is planned in the coming months.

SAMPLE OBJECTIVES

The exercise objectives are as follows:

- Validate Cyber Intrusion Response Plan and Alternate Facility Contingency Plan
- Identify interdependencies, overlaps, and inconsistencies between the two plans
- Validate the team's ability to recover IT operations at alternate facility
- Familiarize staff with their responsibilities under the plans
- Validate the accuracy of recovery procedures documented in the plans
- Coordinate with Federal cyber entities, customers, and key stakeholders
- Identify areas of the plans that need to be revised
- Identify whether additional contingency plans need to be developed.

SAMPLE SCENARIO

[Insert scenario or high-level overview of the scenario.]

SAMPLE EXERCISE FINDINGS

The *[insert exercise name]* provided information on *[insert relevant information]*. An important benefit of the exercise was the opportunity for participants to receive hands-on training in responding to an emergency from the alternate facility. In addition, the exercise provided participants with an opportunity to raise important questions, concerns, and issues. At the conclusion of the exercise, participants were asked to complete an evaluation form regarding the information provided, additional information needed, and their thoughts on the event, to be included in the after action report. *[A sample evaluation form can be found on page D-16.]*

Findings from the exercise and recommended actions are as follows:

General Findings

The exercise provided an excellent opportunity for participants to *[insert relevant information]*. As a result of the exercise, participants left with a heightened awareness of *[insert relevant information]*.

Specific Findings

Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:

Observation 1. [Insert general topic area]

[Insert observation]

Recommendations

[Insert recommendations]

Observation 2. [Insert general topic area]

[Insert observation]

Recommendations

[Insert recommendations]

Example Observations and Recommendations:

Observation 1. Communications

A plan identifying standardized systems for communicating with contingency plan members does not exist.

Recommendations

- The *[insert organization name]* should consider developing a communications plan that establishes standardized communications requirements, addresses how and where backup communication systems will be positioned, and describes procedures for personnel to access backup communication systems.
- The *[insert organization name]* should identify redundant communications systems to ensure that essential personnel can be contacted in the event of an emergency. Redundant communications systems may consist of home telephones, cellular telephones, laptop computers, and other communications systems.

Observation 2. Flyaway Kits

Essential personnel have not been issued flyaway kits, containing personal items and/or those items needed to perform their operations, to carry to relocation facilities in the event of an emergency.

Recommendation

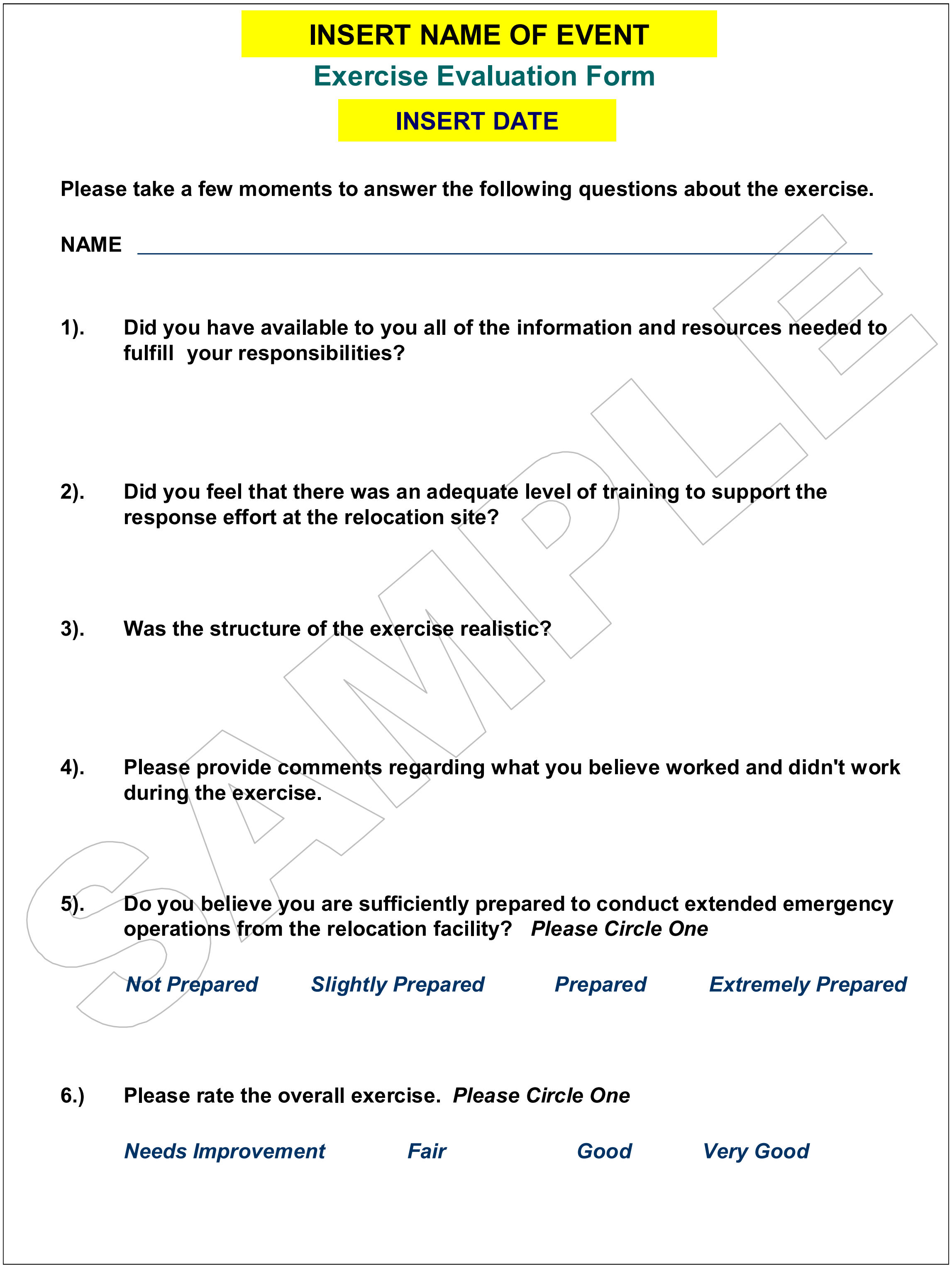
- The *[insert organization name]* should examine the possibility of developing flyaway kits and distributing them in advance to personnel who would relocate during an emergency. In addition to personal items that personnel might need if deployed for an extended period of time, flyaway kits should contain flash drives, diskettes or CD-ROMs with information needed for essential personnel to carry out their essential functions.

SAMPLE SIGN-IN SHEET

Participant Name	Function/Title	Telephone Number/ E-mail Address

SAMPLE EVALUATION FORM

Please take a moment to fill out the evaluation form.



INSERT NAME OF EVENT

Exercise Evaluation Form

INSERT DATE

Please take a few moments to answer the following questions about the exercise.

NAME ____

1). Did you have available to you all of the information and resources needed to fulfill your responsibilities?

2). Did you feel that there was an adequate level of training to support the response effort at the relocation site?

3). Was the structure of the exercise realistic?

4). Please provide comments regarding what you believe worked and didn't work during the exercise.

5). Do you believe you are sufficiently prepared to conduct extended emergency operations from the relocation facility? ***Please Circle One***

Not Prepared ***Slightly Prepared*** ***Prepared*** ***Extremely Prepared***

6.) Please rate the overall exercise. ***Please Circle One***

Needs Improvement ***Fair*** ***Good*** ***Very Good***

SAMPLE EVALUATION RESULTS

Following the *[insert functional exercise name]*, on *[insert date(s)]*, participants were given an evaluation form on which to record their impressions of the exercise. These forms allowed participants to rate presentations on a numerical scale and to provide additional comments for consideration in the after action report. Refer to Exhibit 1 for more detailed information regarding the participants' responses. *[Each exhibit will reflect the evaluation forms for each individual event. If evaluation forms have a point scale, either a pie chart or bar graph will be depicted.]*

The questions covered whether participants thought additional issues should have been raised; whether participants thought the exercise was beneficial; what participants gained from the exercise; and what can be done to improve future exercises. *[Insert percentage]* of the participants completed the evaluation.

In response to the question regarding whether participants thought additional issues should have been raised, nearly *[insert percentage]* of those who completed the evaluation indicated that all relevant issues were addressed. Other comments were *[insert relevant information]*.

In response to the question regarding whether participants thought the exercise was beneficial, *[insert percentage]* of those who completed the evaluation indicated that the exercise was beneficial. Comments ranged from *[insert relevant information (i.e., "good start" to "extremely beneficial.")]*.

In response to the question about what participants gained from the exercise, nearly *[insert percentage]* of those who completed the evaluation form remarked *[insert relevant information]*.

EXHIBIT 1: PARTICIPANT RESPONSES

What are your thoughts on the exercise?	What did you gain from the exercise?
▪ *[Insert comments]* ▪ ▪ ▪	▪ *[Insert comments]* ▪ ▪ ▪

Overall, the feedback from the *[insert functional exercise name]* was *[insert relevant information]*.

Appendix D—Sample Test Documentation

Appendix D provides sample documentation for three types of tests: a component test, a system test, and a comprehensive test. This sample documentation is designed to be used as a template by those responsible for designing and developing test documentation. Templates provided within this section include the following:

- Test Structure Description
- Test Plan
- Test Briefing for Participants
- Test Inject or Action
- Test Validation Worksheet
- Test Evaluation Worksheet
- After Action Report.

D.1 Sample Component Test Documentation

An example of a component test is the occasional test of the nation's Emergency Alert System, formerly known as the Emergency Broadcast Network.[20] During such a test, the equipment is tested, and a tone and announcement associated with an emergency are broadcasted on the radio or television. Although the test does not involve a simulated emergency with responders, the message tests a specific component of the system.

SAMPLE COMPONENT TEST PLAN

[Insert test type or name]

Component Test Plan

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Frequency: *[Insert frequency]*

Test Focus: *[Insert test focus]*

Test Objectives: The objectives of this test are as follows:

- Test the Emergency Broadcast System hardware in a live test environment
- Identify any delays, failures or areas for improvement

Test Details: *[Insert test details]*

Participants: *[Insert participants]*

Training Staff: *[Insert training staff]*

Validation Staff: *[Insert validation staff]*

Evaluation Staff: *[Insert evaluation staff]*

Test Cancellation Procedures: *[Insert test cancellation procedures]*

Test Main Point of Contact: *[Insert test main point of contact]*

Test Approval Grantor: *[Insert test approval grantor]*

[20] For more information on the Emergency Alert System, visit http://www.fcc.gov/eb/eas/.

SAMPLE COMPONENT TEST BRIEFING FOR PARTICIPANTS

On *[insert date]* between *[insert time]* and *[insert time]*, the *[insert component]* for *[organization or policy]* will be tested. Participants will be expected to perform the following tasks:

- *[Insert task]*
- *[Insert task]*

Test Cancellation Procedures: *[Insert test cancellation procedures]*

If you have any questions, please contact *[insert point of contact]*.

SAMPLE COMPONENT TEST INJECT OR ACTION

Initiate the Emergency Alert System, which will perform the following functions:

- Discontinue normal programming.
- Broadcast the following message: *"This is a test. This station [optional—insert station call sign] is conducting a test of the Emergency Broadcast System. This is only a test."*
- Transmit the two-tone attention signal from the EBS encoder.
- Broadcast the following message: *"This is a test of the Emergency Alert System. The broadcasters of your area in voluntary cooperation with the Federal, state and local authorities have developed this system to keep you informed in the event of an emergency. If this had been an actual emergency, [optional—stations may mention the types of emergencies likely to occur in their area] the Attention Signal you just heard would have been followed by official information, news or instructions. This station [optional—insert station call sign] serves the [insert operational area name] area. This concludes this test of the Emergency Alert System."*

SAMPLE COMPONENT TEST VALIDATION

A test of a component requires validation criteria to determine whether the component or system functioned as intended. Test validation should include the metrics by which the success of the component or system will be measured. It should also detail the expected outcome; in this case, the two-tone attention signal and message should be heard clearly.

SAMPLE COMPONENT TEST VALIDATION WORKSHEET

[Insert test type or name]

Component Test Validation Worksheet

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Test Focus: *[Insert test focus]*

Participants: *[Insert participants]*

Training Staff: *[Insert training staff]*

Validation Staff: *[Insert validation staff]*

Test Objectives: The objectives of this test are as follows:

- Test the Emergency Broadcast System hardware in a live test environment
- Identify any delays, failures or areas for improvement

Validation Methodology: *[Insert validation methodology]*

Was the test able to be validated? *[Insert answer]*

Comments: *[Insert comments]*

Were there any aspects of the test that could not be validated? *[Insert answer]*

Comments: *[Insert comments]*

Recommendations: *[Insert recommendations]*

SAMPLE COMPONENT TEST EVALUATION

Based on the objectives and validation metrics, the test should be evaluated to determine whether the system test and associated components and processes performed adequately. Possible improvements and recommendations are an important part of the evaluation process.

SAMPLE EVALUATION WORKSHEET

[Insert test type or name]

Component Test Evaluation Worksheet

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Test Focus: *[Insert test focus]*

Participants: *[Insert participants]*

Training Staff: *[Insert training staff]*

Validation Staff: *[Insert validation staff]*

Evaluation Staff: *[Insert evaluation staff]*

Test Objectives: The objectives of this test are as follows:

- Test the Emergency Alert System hardware in a live test environment
- Identify any delays, failures or areas for improvement

Were the test objectives met? *[Insert answer]*

Comments: *[Insert comments]*

Test details: *[Insert test details]*

Was testing criterion adequate? *[Insert answer]*

Comments: *[Insert comments]*

Could the testing criterion be improved? *[Insert answer]*

Comments: *[Insert comments]*

Was the test validation criterion adequate? *[Insert answer]*

Could the test validation criterion be improved? *[Insert answer]*

Comments: *[Insert comments]*

Did the test perform as expected? *[Insert answer]*

Comments: *[Insert comments]*

Were there any failures during the test? *[Insert answer]*

Did the failure cause the test to fail? *[Insert answer]*

Comments: *[Insert comments]*

Recommendations: *[Insert recommendations]*

COMPONENT TEST AFTER ACTION REPORT

The After Action Report should consist of the following components:

- General findings, often in the form of an executive summary

- Specific findings
- Supporting data.

COMPONENT TEST GENERAL FINDINGS

The General Findings section highlights the outcome of the test. It might consist of a statement along the lines of the following:

> The component test provided an excellent opportunity for participants to test the *[insert relevant information]*. As a result of this component test, participants received a heightened awareness of the importance of *[insert relevant information]*. The *[organization or department]* as a whole learned *[insert relevant information]* as a result of this test.

COMPONENT TEST SPECIFIC FINDINGS

The Specific Findings section provides greater detail of the results of the test. It should provide sufficient detail so that a person knowledgeable of the technical aspects of the component could use the evaluation to improve the component or process. A possible outline for the specific observations section is as follows:

> Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:
>
> **Observation 1.** ***[Insert general topic area]***
>
> *[Insert observation]*
>
> **Recommendations**
>
> *[Insert recommendations]*
>
> **Observation 2.** ***[Insert general topic area]***
>
> *[Insert observation]*
>
> **Recommendations**
>
> *[Insert recommendations]*

SUPPORTING DATA

The Supporting Data section of the report includes the specific data that was collected during the test. These are often included as attachments with a brief explanation of how they were gathered.

D.2 Sample System Test Documentation

An example of a system test is the testing of an organization's data backup and restoration system and procedures. During such a test, all aspects of the data backup equipment and personnel procedures for archiving and restoring data are tested.

SAMPLE SYSTEM TEST STRUCTURE:

System Test: Data Backup and Restoration

- Test data backup procedure
- Test data backup equipment
- Test data backup integrity verification procedures
- Test local data storage procedures
- Test local data retrieval procedures
- Test offsite data storage procedures
- Test offsite data retrieval procedures
- Test data restoration for UNIX systems
- Test data restoration for Microsoft Systems
- Test data restoration for network systems
- Test data restoration for other systems.

SAMPLE SYSTEM TEST PLAN

[Insert test type or name]

System Test Plan

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Frequency: *[Insert frequency]*

Test Focus: *[Insert test focus]*

Test Objectives: *[Insert test objectives]*

Test Details: *[Insert test details]*

Test Components:

- *[Insert component]*
- *[Insert component]*
- *[Insert component]*

System Test Component 1: *[Insert component]*[21]

- **Component Test Participants:** *[Insert participants]*
- **Component Test Validation Staff:** *[Insert validation staff]*
- **Component Test Evaluation Staff:** *[Insert evaluation staff]*
- **Component Test Cancellation Procedures:** *[Insert test cancellation procedures]*
- **Component Test Main Point of Contact:** *[Insert test main point of contact]*
- **Component Test Approval Grantor:** *[Insert test approval grantor]*

System Test Main Point of Contact: *[Insert system test main point of contact]*

System Test Approval Grantor: *[Insert system test approval grantor]*

SAMPLE SYSTEM TEST BRIEFING FOR PARTICIPANTS

On *[insert date]* between *[insert time]* and *[insert time]*, the *[insert component or system]* for *[department or policy]* will be tested. Each of the following components will be tested:

- *[Insert component]*. Date: *[insert date]*. Time: *[insert time]* to *[insert time]*.
- *[Insert component]*. Date: *[insert date]*. Time: *[insert time]* to *[insert time]*.

[insert component] Component Test in *[insert system]* System Test[22]

On *[insert date]* between *[insert time]* and *[insert time]*, the *[insert component]* for *[department or policy]* will be tested. Participants will be expected to perform the following tasks:

- *[Insert task]*
- *[Insert task]*

Test Cancellation Procedures: *[Insert test cancellation procedures]*

If you have any questions, please contact *[insert point of contact]*.

[21] Repeat this sub-section as needed for each component test within the system test.

[22] Repeat this sub-section as needed for each component test within the system test.

SAMPLE SYSTEM TEST VALIDATION

A test of any system requires methods and criteria to evaluate whether the system test and associated component tests or processes worked as intended. Test validation should include the metrics by which the success of the component or process will be measured and detail the expected outcome. System test validation can be determined by the validation of each individual component test objectives and validation.

In this example, validation for this system test should verify the backup procedures' accuracy and equipment functionality for backing up data for its associated type of systems; verify data integrity checking; validate local and offsite data storage and retrieval procedures; and verify system restoration function as expected for each associated type of system.

SAMPLE SYSTEM TEST VALIDATION WORKSHEET

[Insert test type or name]

System Test Validation Worksheet

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Test Focus: *[Insert test focus]*

Participants: *[Insert participants]*

Training Staff: *[Insert training staff]*

Validation Staff: *[Insert validation staff]*

Test Objectives: The objectives of this test are as follows:

- *[Insert objective]*
- *[Insert objective]*

Test Components: *[Insert test components]*

Validation Methodology: *[Insert validation methodology]*

Was the test able to be validated? *[Insert answer]*

Comments: *[Insert comments]*

Were there any components of the test that could not be validated? *[Insert answer]*

Comments: *[Insert comments]*

Recommendations: *[Insert recommendations]*

SAMPLE SYSTEM TEST EVALUATION

Based on the objectives and validation metrics, the test should be evaluated to determine whether the system test and associated components and processes performed adequately. Possible improvements and recommendations are an important part of the evaluation process.

SAMPLE EVALUATION WORKSHEET

[Insert test type or name]

System Test Evaluation Worksheet

Date of Testing: *[Insert date]*

Time Period: *[Insert time] to [insert time]*

Test Focus: *[Insert test focus]*

Participants: *[Insert participants]*

Training Staff: *[Insert training staff]*

Validation Staff: *[Insert validation staff]*

Evaluation Staff: *[Insert evaluation staff]*

Test Components: *[Insert test components]*

Test Objectives: The objectives of this test are as follows:

- *[Insert objective]*
- *[Insert objective]*

Were the test objectives met? *[Insert answer]*

Comments: *[Insert comments]*

Test details: *[Insert test details]*

Was testing criterion adequate? *[Insert answer]*

Comments: *[Insert comments]*

Could the testing criterion be improved? *[Insert answer]*

Comments: *[Insert comments]*

Was the test validation criterion adequate? *[Insert answer]*

Could the test validation criterion be improved? *[Insert answer]*

Comments: *[Insert comments]*

Did the test perform as expected? *[Insert answer]*

Comments: *[Insert comments]*

Did any test components fail? *[Insert answer]*

Did the failure cause the test to fail? *[Insert answer]*

Comments: *[Insert comments]*

Recommendations: *[Insert recommendations]*

SYSTEM TEST AFTER ACTION REPORT

A system after action report should consist of the following components:

- General findings, often in the form of an executive summary
- Specific findings
- Supporting data.

SYSTEM TEST GENERAL FINDINGS

The General Findings section highlights the outcome of the system test. It might consist of a statement along the lines of the following:

> The system test provided an excellent opportunity for participants to *[insert relevant information]*. As a result of the test, participants received a heightened awareness of the importance of *[insert relevant information]*. The *[organization or department]* as a whole learned *[insert relevant information]* as a result of this test.

SYSTEM TEST SPECIFIC FINDINGS

The Specific Findings section provides greater detail of the results of the test. It should provide sufficient detail so that a person knowledgeable of the technical aspects of the component could use the evaluation to improve the component or process. A possible outline for the specific observations section is as follows:

> Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:
>
> **Observation 1. [Insert general topic area]**
>
> *[Insert observation]*

Recommendations

[Insert recommendations]

Observation 2. [Insert general topic area]

[Insert observation]

Recommendations

[Insert recommendations]

SUPPORTING DATA

The Supporting Data section of the report includes the specific data that was collected during the test. These are often included as attachments with a brief explanation of how they were gathered. For example, individual component testing forms might be attached as supporting data.

D.3 Sample Comprehensive Test Documentation

An example of a comprehensive test is the testing of all the systems and components comprising an organization's business continuity plan. During such a test, all the equipment, processes, and procedures for each system and associated components are tested as a comprehensive unit.

SAMPLE COMPREHENSIVE TEST PLAN OVERVIEW

Because a comprehensive test plan is specifically designed around an organization's security, business continuity, or other plans, it is not practical to provide a full sample of the test documents. However, this section provides a plan overview that outlines the systems and component tests as part of the comprehensive plan. The forms in Sections D.1 and D.2 for component and system testing can be used to form individual parts of the comprehensive test.

SAMPLE COMPREHENSIVE TEST STRUCTURE

Comprehensive Tests are comprised of several System Tests which in turn are comprised of several Component Tests. The following is an example of the structure of one branch of a comprehensive test.

Comprehensive Test: Business Continuity Plan

- **System Test:** Data Backup and Restoration
  - **Component Test:** Test data backup procedure
  - **Component Test:** Test data backup equipment
  - **Component Test:** Test data backup integrity verification procedures
  - **Component Test:** Test local data storage procedures
  - **Component Test:** Test local data retrieval procedures
  - **Component Test:** Test offsite data storage procedures
  - **Component Test:** Test offsite data retrieval procedures
  - **Component Test:** Test data restoration for UNIX systems
  - **Component Test:** Test data restoration for Microsoft systems
  - **Component Test:** Test data restoration for network systems
  - **Component Test:** Test data restoration for other systems
  - **Component Test:** Identify any delays, failures, or areas of improvement.

SAMPLE COMPREHENSIVE TEST PLAN

[Insert test type or name]

Comprehensive Test Plan

Dates of Testing: *[Insert date]* to *[insert date]*

Time Period: *[Insert time] to [insert time]*

Frequency: *[Insert frequency]*

Test Focus: *[Insert test focus]*

Test Objectives: *[Insert test objectives]*

Test Details: *[Insert test details]*

Systems to be Tested:

- *[Insert system test]*
- *[Insert system test]*
- *[Insert system test]*

System 1: *[Insert system test]*[23]

System 1 Component Tests:

- *[Insert component test item]*
- *[Insert component test item]*
- *[Insert component test item]*

Component Test 1: *[Insert component]*[24]

- Component Test Participants: *[Insert participants]*
- Component Test Validation Staff: *[Insert validation staff]*
- Component Test Evaluation Staff: *[Insert evaluation staff]*
- Component Test Cancellation Procedures: *[Insert test cancellation procedures]*
- Component Test Main Point of Contact: *[Insert test main point of contact]*
- Component Test Approval Grantor: *[Insert test approval grantor]*

Comprehensive Test Cancellation Procedures: *[Insert test cancellation procedures]*

Comprehensive Test Main Point of Contact: *[Insert test main point of contact]*

Comprehensive Test Approval Grantor: *[Insert test approval grantor]*

[23] Repeat this sub-section as needed for each system test within the comprehensive test.

[24] Repeat this sub-section as needed for each component test within each system test.

SAMPLE COMPREHENSIVE TEST VALIDATION

A comprehensive test of many systems and system components requires a method and criteria to evaluate whether the component or process worked as intended. Because a comprehensive test is a compilation of many system and component tests, the validation can be determined from the validation of the system and component, and evaluated as a whole.

Comprehensive test validation should include the metrics by which the success of the component or process will be measured. It should detail the expected outcome.

SAMPLE COMPREHENSIVE TEST EVALUATION

Based on the objectives and validation metrics, the test should be evaluated to determine whether the comprehensive test and its associated system and component tests performed adequately. Because a comprehensive test is a compilation of system and component tests, the comprehensive test will be determined from the evaluations of the individual system and, and then evaluated as a whole. Possible improvements and recommendations are an important part of the evaluation process.

COMPREHENSIVE TEST AFTER ACTION REPORT

A comprehensive test after action report should consist of the following components:

- General findings, often in the form of an executive summary
- Specific findings
- Supporting data.

COMPREHENSIVE TEST GENERAL FINDINGS

The General Findings section highlights the outcome of the test. It might consist of a statement along the lines of the following:

> The test provided an excellent opportunity for participants to *[insert relevant information]*. As a result of the test, participants received a heightened awareness of the importance of *[insert relevant information]*. The *[organization or department]* as a whole learned *[insert relevant information]* as a result of this test.

COMPREHENSIVE TEST SPECIFIC FINDINGS

The Specific Findings section provides greater detail of the results of the test. It should provide sufficient detail so that a person knowledgeable of the technical aspects of the component could use the evaluation to improve the component or process. A possible outline for the specific observations section is as follows:

> Specific observations made during the exercise, and recommendations for enhancement of the plan, are as follows:
>
> **Observation 1. *[Insert general topic area]***

[Insert observation]

Recommendations

[Insert recommendations]

Observation 2. ***[Insert general topic area]***

[Insert observation]

Recommendations

[Insert recommendations]

SUPPORTING DATA

The Supporting Data section of the report includes the specific data that was collected during the test. These will often be included as attachments with a brief explanation of how they were gathered.

Appendix E—Glossary

Appendix E contains definitions for technical terms related to TT&E.

After Action Report (AAR): Document containing findings and recommendations from tabletop and functional exercises.

After Action Summary: Document that captures and summarizes the information obtained from the evaluation or critique forms following a training event.

Component Test: Test of individual hardware and software elements or groups of related elements.

Comprehensive Test: Test of a complete organizational plan, such as a contingency, incident response, or infrastructure protection plan.

Conduct Phase: The TT&E phase during which the TT&E event is carried out.

Controllers: Functional exercise staff members responsible for monitoring, managing, and controlling exercise activity to meet established objectives.

Data Collectors: Tabletop and functional exercise staff members who are provided forms specifically designed for their role in the exercise and record information about actions that occur during the exercise or that should occur but do not.

Design Phase: The TT&E phase during which teams are established, the training, exercise, or test topic and scope are determined, the objectives and participants are identified, and the event logistics are coordinated.

Development Phase: The TT&E phase during which the TT&E program coordinator works with the design teams to develop all documentation necessary for the conduct of the TT&E event, including the documentation to be used before, during, and after the event.

Evaluation Phase: The TT&E phase during which participants complete an evaluation or critique form on the success of the TT&E event, lessons learned from the event are analyzed and documented in an after action report or summary, and future TT&E events or sessions are modified as needed.

Exercise Briefings: Material that is presented to participants during the exercise to outline the agenda, objectives, scenario, and other relevant information.

Facilitator Guides: A document for exercise facilitators consisting of an agenda, curriculum, exercise scope, exercise objectives, scenarios, and sample discussion questions (if applicable). Additionally, facilitator guides include talking points, curriculums, discussion points, and other materials to aid facilitators.

Facilitator: Tabletop exercise staff member that serves in a leadership role to help guide participants' discussion and ensure exercise objectives are met.

Functional Exercise: Exercise that uses simulated emergencies to exercise specific team members, procedures, and assets involved in one or more functional aspects of a plan.

Functional Exercise Design Team: Team that determines the exercise topic based on the plan being exercised and coordinates the development of functional exercise material.

Injects/Implementers: Individual action items based on the higher-level MSELs that are assigned by control staff to participants during an exercise.

Instructional Design Team: Team that coordinates the development of the curriculum; briefings; participant manuals; and instructor guides for a training event.

Instructional Strategy: Instructional strategies, designed by the instructional design team, effectively and efficiently lead trainee performances. Strategies include sequencing of performance objectives; identifying pre-instructional materials, testing and validating processes, and identifying follow-on activities; determining how the content is presented; and determining participation activities. To ensure transfer of knowledge, skills, or abilities, training events consist of 1/3 presentation and 2/3 activities.

Master Scenario Events List (MSEL): High-level scenarios to be implemented during an exercise.

Participant Guides: Document consisting of an agenda, curriculum, exercise scope, exercise objectives, scenarios, and sample discussion questions (if applicable).

Plan Coordinator: Person responsible for all aspects of planning, including the TT&E element of maintaining the plans. The plan coordinator has overall responsibility for the plan, including development, implementation, and maintenance.

Simulators: Functional exercise staff members who simulate or represent non-participating individuals and organizations whose input or participation is necessary to the flow of the exercise.

System Test: Test performed on a complete system to evaluate its compliance with specified requirements.

Tabletop Exercise: Exercise based on a facilitator guiding participants through a discussion centered on a single scenario or multiple scenarios, with the intent to meet pre-defined objectives.

Tabletop Exercise Design Team: Team that determines the exercise topic based on the plan being exercised and coordinates the development of briefing materials; facilitator and participant guides; and the evaluation criteria to be used when developing the after action report for a tabletop exercise.

Test: An evaluation tool that uses quantifiable metrics or expected outcomes to assess the operability of an IT system or IT system component that is identified as critical in one of an organization's plans, in as close to an operational environment as possible.

Test Design Team: Team that determines the test topic based on the system being exercised and coordinates the development of a test plan, test scripts, and evaluation criteria.

Test Scripts: Specific instructions used to assess the functionality of a particular component or system.

Test, Training, and Exercise (TT&E) Program: A means for ensuring select personnel are trained in their roles and responsibilities; plans are exercised to validate their viability; and systems are tested to validate their operability.

Tracking Forms: Document to be used for capturing the results of training, exercises, or tests.

Training: Informing participants of their roles and responsibilities within the plan being exercised, thereby preparing them for tests, exercises, and actual emergency situations.

TT&E Plan: Plan developed to facilitate establishing a comprehensive TT&E program, which outlines all elements of the program, and ensures information surrounding the program is documented.

TT&E Policy: Policy that outlines the organization's internal and external requirements associated with training personnel, exercising plans, and testing systems.

TT&E Program Coordinator: Person who works with the plan coordinator to determine the training, exercise, or test topic and scope based on the current needs of the organization.

This page has been left blank intentionally.

Appendix F—Acronyms

Selected acronyms used in the guide are defined below.

AAR	After Action Report
AF	Alternate Facility
BCP	Business Continuity Plan
CD	Compact Disk
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
COOP	Continuity of Operations
EXPLAN	Exercise Plan
FISMA	Federal Information Security Management Act
FPC	Federal Preparedness Circular
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
ITL	Information Technology Laboratory
MSEL	Master Scenario Events List
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SME	Subject Matter Expert
SP	Special Publication
TT&E	Test, Training, and Exercise
UTSA	University of Texas-San Antonio

This page has been left blank intentionally.

Appendix G—Print and Online Resources

Appendix G identifies print and online resources that may be helpful to the reader in scoping, planning, documenting, conducting, and evaluating IT exercises.

- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 2001. http://www.fas.org/irp/offdocs/eo/eo-13231.htm
- Federal Emergency Management Agency, Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations*, June 15, 2004. http://www.fema.gov/pdf/library/fpc65_0604.pdf
- Federal Information Security Management Act of 2002, *Public Law 107-347*, December 2002. http://csrc.nist.gov/policies/FISMA-final.pdf
- Homeland Security Exercise and Evaluation Program, May 2004. http://www.ojp.usdoj.gov/odp/docs/HSEEPv3.pdf
- NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-18, *Guide for Developing Security Plans and Information Technology Systems*, December 1998. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003. http://csrc.nist.gov/publications/nistpubs/index.html
- NIST SP 800-61, *Computer Security Incident Handling Guide*, January 2004. http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
- Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Systems*, February 8, 1996. http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
- Presidential Decision Directive 63, *Protecting America's Critical Infrastructures*, May 22, 1998. http://www.fas.org/irp/offdocs/pdd/index.html
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government*, October 21, 1998. http://www.fas.org/irp/offdocs/pdd/index.html